Normal bisimulations in process calculi with passivation

Sergueï Lenglet, Alan Schmitt, Jean-Bernard Stefani

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Normal bisimulations in process calculi with passivation

Sergueï Lenglet, Alan Schmitt, Jean-Bernard Stefani

N° 6664

September 2008

Thème COM

Rapport de recherche

SN 0249-6399 ISRN INRIA/RR--6664--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
GRENOBLE - RHÔNE-ALPES

Normal bisimulations in process calculi with passivation

Sergueï Lenglet, Alan Schmitt, Jean-Bernard Stefani

Thème COM — Systèmes communicants
Équipes-Projets SARDES

Rapport de recherche n° 6664 — September 2008 — 102 pages

Abstract: Behavioral theory for higher-order process calculi is less well developed than for first-order ones such as the π-calculus. The most natural process equivalence relation, barbed congruence, is difficult to use in practice because of the infinite number of test contexts it requires. One is therefore lead to find simpler characterizations of barbed congruence, which may not be easy to do for higher-order process calculi, especially in the weak case. Such characterizations have been obtained for some calculi. For instance, in the case of the higher π-calculus, HOπ, Sangiorgi has defined a notion of *normal* bisimulation, which characterizes barbed congruence and that requires only a finite number of tests. In this paper, we study bisimulations in higher-order calculi with a passivation operator, that allows the interruption and thunkification of a running process. We develop a normal bisimulation that characterizes barbed congruence, in the strong and weak cases, in a higher-order calculus with passivation, but without name restriction. We then show that this characterization result does not hold in the presence of name restriction.

Key-words: Process calculus, higher-order, behavioral theory, barbed congruence, normal bisimulation

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

Bisimulations normales dans des calculs de processus avec passivation

Résumé : La théorie comportementale des calculs de processus d'ordre supérieur est moins développée que celle des calculs du premier ordre tels que le π-calcul. La relation d'équivalence entre processus la plus naturelle, la congruence barbée, est difficile à utiliser en pratique à cause du nombre infini de contextes de test qu'elle requiert. On est donc conduit à chercher des caractérisations plus simples de l'équivalence barbée, qui ne sont pas faciles à obtenir dans des calculs d'ordre supérieur, notamment dans le cas faible. De telles caractérisations ont pu être trouvées pour quelques calculs. Par exemple, pour le π-calcul d'ordre supérieur, HOπ, Sangiorgi a défini une notion de *bisimulation normale*, qui caractérise la congruence barbée et qui ne nécessite qu'un nombre fini de contextes de test. Dans ce rapport, nous étudions diverses formes de bisimulations dans des calculs d'ordre supérieur avec un opérateur de passivation qui autorise l'interruption et la sérialisation d'un processus en cours d'exécution. Nous définissons une bisimulation normale qui caractérise la congruence barbée, dans le cas fort et le cas faible, dans un calcul d'ordre supérieur avec passivation mais sans restriction. Nous montrons ensuite que cette caractérisation ne tient plus en présence de restriction.

Mots-clés : Calcul de processus, ordre supérieur, théorie comportementale, congruence barbée, bisimulation normale

Contents

1 Introduction

Motivation

A natural notion of behavioral equivalence for process calculi is *barbed congruence*. Informally, two processes are barbed-congruent if they behave in the same way (i.e., they have the same reductions and the same observables), when placed in similar, but arbitrary, contexts. Due to this quantification on contexts, barbed congruence is unwieldy to use for proofs of equivalence, or to serve as a basis for automated verification tools. One is thus lead to study coinductive characterizations of barbed congruence, typically in the form of bisimilarity relations.

For first-order process calculi, such as the π-calculus and its variants, the resulting behavioral theory is well developed, and one can in general readily define bisimularity relations that characterize barbed congruence for these calculi. For higher-order process calculi, the situation is less satisfactory. Simple higher-order calculi, such as HOπ [12, 13], have a well-studied behavioral theory. For HOπ, Sangiorgi has defined *context* and *normal* bisimilarity relations, which are both sound with respect to barbed congruence (i.e. they are included in barbed congruence), and sometimes complete (i.e. they contain barbed congruence), leading to a full characterization. Context bisimilarity still involves some quantification over test contexts. For instance, for assessing the equivalence of two processes which consist only of the output of a message on a communication channel a, context bisimilarity needs to consider every interacting system that is capable of doing an input on channel a. Normal bisimilarity improves context bisimilarity by requiring only a single test context. E.g., in the case of two emitting processes, as above, normal bisimilarity only requires to compare the behavior of the two processes when placed in parallel with a single, particular receiving process. Furthermore, context and normal bisimilarities characterize barbed congruence both in the strong case (where a step from the first process must be simulated by a single step of the second process), and in the weak case (where a step of a first process must be simulated by a single step of the second process, possibly preceded and/or followed by an arbitrary number of internal steps).

Unfortunately, HOπ is not expressive enough to faithfully model concurrent systems with dynamic reconfiguration or strong mobility capabilities. For instance, a running HOπ process cannot be stopped, which prevents the faithful modeling of process failures, of online process replacement, or strong process mobility. It is for this reason that we have seen the emergence of process calculi with (forms of) *process passivation*. Process passivation allows a named process to be stopped and its state captured at any time during its execution. The Kell calculus [16] and Homer [8] are examples of higher-order process calculi with passivation. The behavioral theory of these calculi is less understood than the one for HOπ, whose proof techniques and relations do not easily carry over. More precisely, no sound and complete characterization of barbed congruence has been found in the weak case. In the strong case, context bisimilarities have been defined. They characterize barbed congruence at the expense of larger test contexts than in the case of context bisimilarity for HOπ. Importantly, no relation akin to normal bisimilarity has been found for these calculi.

Contributions

To pinpoint issues that arise in the development of a behavioral theory for higher-order calculi with passivation, and to show that they arise from the interplay between passivation and restriction, we consider in this paper two calculi with passivation, which are simpler than both Homer and the Kell calculus, and which differ merely in the presence of restriction. The first one, called HOP, extends HOcore with passivation and sum. HOcore is a minimal higher-order concurrent calculus without restriction that has recently been studied in [9]. As a first contribution, we show that HOP admits a sound and complete form of normal bisimulation, in both the strong and weak cases. The second calculus, called HOπP, extends HOπ with passivation. As a second contribution, we show that with HOπP a large class of tests do not suffice to build a sound normal bisimulation. This casts some doubt as to whether a suitable notion of normal bisimilarity, that is with finite testing, can be found for HOπP, and therefore for Homer and the Kell calculus.

Organization of the report

The report is organized as follows: in Section 2, we quickly recall the syntax, semantics, and behavioral theory of HOπ. In Section 3, we define a calculus called HOπP that extends HOπ with passivation. We propose behavioral equivalences inspired by previous works on Homer and the Kell-calculus, and we give characterization results for HOπP, that mirror those obtained for Homer and for the Kell calculus. This allows us to review the proof techniques developed for Homer and for the Kell calculus. The main contribution of this paper is in Section 4, where we define context and normal bisimilarities that characterize barbed congruence for HOP. We prove that these relations are not suitable in HOπP in Section 5, and we show that a large class of finite test processes cannot be used as a basis for defining a form of normal bisimilarity for HOπP. We discuss related work in Section 6, and Section 7 concludes the paper. Complete proofs are given in the appendices. Appendices A to C and Appendix G give details and proofs for HOπP, while Appendices D to F deal with HOP.

2 Bisimulations in HOπ

In this section, we recall some results on bisimulations in a higher-order calculus HOπ [13]. We base our work on this calculus since it enjoys a nice behavioral theory and is very close to the calculi with passivation we wish to study.

Notations:

- X, Y, Z: process variables
- $m, n, \overline{m}, \overline{n}$: first-order names
- $l \in \{m, \overline{m}\} \cup \tau$
- $a, b, \overline{a}, \overline{b}$: higher-order names
- x, y: channel names (first-order or higher-order names)
- $\widetilde{x}$: vectors of channel names $x_1, \ldots, x_n$

Syntax:

$$P ::= \mathbf{0} \;\mid\; X \;\mid\; P \mid P \;\mid\; l.P \;\mid\; a(X)P \;\mid\; \overline{a}\langle P\rangle P \;\mid\; \nu x.P \;\mid\; !P$$

Figure 1: Syntax of the Higher-Order π

2.1 Syntax and Semantics of HOπ

The calculus HOπ [13] extends the π-calculus with higher-order communication, which allows processes as arguments in messages. The syntax of the calculus and some notations can be found in Figure 1. The constructs of the calculus are:

- The inactive process $\mathbf{0}$.
- Process variables X.
- Parallel composition of two processes $P \mid Q$.
- Prefixed processes $\tau.P$: this process can perform an internal action τ before continuing as P.
- CCS-like first-order communication $m.P \mid \overline{m}.P$, where no information is exchanged, that allows synchronization between processes.
- Synchronous higher-order communication $a(X)P \mid \overline{a}\langle Q\rangle R$: the left process $a(X)P$ is waiting for a process (here Q) on name a, and then continues as $P\{Q/X\}$. The right process $\overline{a}\langle Q\rangle R$ sends the process Q on a and then continues as R. In process $a(X)P$, the variable X is bound. We write $\mathrm{fv}(P)$ the free variables of a process P.
- Name restriction $\nu x.P$, where the (first-order or higher-order) name x is made local to the process P. In process $\nu x.P$, the name x is bound. We write $\mathrm{bn}(P)$ (resp $\mathrm{fn}(P)$) the bound names (resp free names) of a process P.
- Process replication $!P$, which provides an infinite number of copies of P.

$$l.P \xrightarrow{l} P \ \text{LTS-Prefix} \qquad a(X)P \xrightarrow{a} (X)P \ \text{LTS-Abstr}$$

$$\overline{a}\langle Q\rangle P \xrightarrow{\overline{a}} \langle Q\rangle P \ \text{LTS-Concr} \qquad \frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q} \ \text{LTS-Par}$$

$$\frac{P \xrightarrow{\alpha} A \qquad \alpha \notin \{x, \overline{x}\}}{\nu x.P \xrightarrow{\alpha} \nu x.A} \ \text{LTS-Restr} \qquad \frac{P \xrightarrow{\alpha} A}{!P \xrightarrow{a} A \mid !P} \ \text{LTS-Replic}$$

$$\frac{P \xrightarrow{m} P' \qquad Q \xrightarrow{\overline{m}} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'} \ \text{LTS-FO} \qquad \frac{P \xrightarrow{m} P_1 \qquad P \xrightarrow{\overline{m}} P_2}{!P \xrightarrow{\tau} P_1 \mid P_2 \mid !P} \ \text{LTS-Replic-FO}$$

$$\frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \ \text{LTS-HO} \qquad \frac{P \xrightarrow{a} F \qquad P \xrightarrow{\overline{a}} C}{!P \xrightarrow{\tau} F \bullet C \mid !P} \ \text{LTS-Replic-HO}$$

Figure 2: Labelled transition system for HOπ

We identify processes up to α-conversion of names and variables. For convenience, we sometimes identify a name vector $\widetilde{x} = x_1, \dots, x_n$ with its supporting set $\{x_1, \dots, x_n\}$ (assuming the x_i are mutually distinct).

Remark 1. *Replication may be encoded with the other constructs. We first write $!P$ with a prefix: $\nu m.(\overline{m}.\mathbf{0} \mid !m.(P \mid \overline{m}.\mathbf{0}))$. To have a copy of process P, we just have to take a copy of $m.(P \mid \overline{m}.\mathbf{0})$ and trigger the communication on m.*

Consequently, it is enough to encode replication of prefixed processes. Let $Y = m.t(X)(P \mid X \mid \overline{t}\langle X\rangle\mathbf{0})$. We encode $!m.P$ by $Q = \nu t.(\overline{t}\langle Y\rangle\mathbf{0} \mid Y)$. The process Y is similar to a copy of $m.P$, except that it is waiting for a copy of itself on t after a communication on m, to launch a copy of P and to recreate the process Q. Hence the process Q reduces to $P \mid Q$ after a communication on m, like the process $!m.P$.

However this encoding raises issues with strong behavioral equivalences, hence we keep replication explicitly in the calculus.

The semantics of the calculus may be based on a reduction relation $\longrightarrow$, defined modulo a structural congruence relation $\equiv$, or may be derived from a labeled transition system (LTS) semantics $\xrightarrow{\alpha}$. We only recall the LTS semantics in the following subsection. The reduction relation (for HOπ as well as all the calculus in this paper) can be recovered from the structural congruence and the labeled transition system relation via the equation $\longrightarrow \,=\, \equiv\xrightarrow{\tau}\equiv$.

2.2 Labeled Transition Semantics

We present here a labelled transition system (LTS) semantics for HOπ in the style of [11]. In the LTS semantics, we have three kind of possible evolutions for processes:

- First-order evolution labeled by l, where a process evolves toward a process.
- Message input on a channel a, where a process evolves toward an *abstraction* $(X)Q$. The transition $P \xrightarrow{a} (X)Q$ means that the process P may receive a process R on the name a to continue as $Q\{R/X\}$.
- Message output on a channel a, where a process evolves toward a *concretion* $\nu\widetilde{x}.\langle R\rangle Q$, where $\widetilde{x} \subseteq \mathrm{fn}(R)$. The transition $P \xrightarrow{\overline{a}} \nu\widetilde{x}.\langle R\rangle Q$ means that the process P may send the process R on the name a and continue as Q, and the scope of names $\widetilde{x}$ has to be expanded to encompass the recipient of R. We write $\mathrm{bn}(C) = \widetilde{x}$ the bound names of a concretion.

A higher-order communication takes place when a concretion interacts with an abstraction. We define a pseudo-application operator $\bullet$ between an abstraction $F = (X)P$ and a concretion $C = \nu\widetilde{x}.\langle R\rangle Q$ by:

$$(X)P \bullet \nu\widetilde{x}.\langle R\rangle Q \triangleq \nu\widetilde{x}.(P\{R/X\} \mid Q) \qquad \mathrm{fn}(P) \cap \widetilde{x} = \emptyset$$

The rule for higher-order communication on name a is:

$$\frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C}\ \text{LTS-HO}$$

Let the set of *agents*, noted A, be the set of processes, abstractions and concretions. A process always evolves toward an agent. Rules LTS-Par and LTS-Restr require the extension of the parallel composition and restriction operators to all agents:

- Let $F = (X)Q$
  - If $X \notin \mathrm{fv}(P)$, then $F \mid P$ stands for $(X)(Q \mid P)$ and $P \mid F$ stands for $(X)(P \mid Q)$.
  - $\nu x.F = (X)\nu x.P$.
- Let $C = \nu\widetilde{y}.\langle Q\rangle R$
  - If $\widetilde{y} \cap \mathrm{fn}(P) = \emptyset$, then $C \mid P$ stands for $\nu\widetilde{y}.\langle Q\rangle(R \mid P)$, and $P \mid C$ stands for $\nu\widetilde{y}.\langle Q\rangle(P \mid R)$.
  - If $x \in \mathrm{fn}(Q)$, then $\nu x.C = \nu\widetilde{y}, x.\langle Q\rangle R$. Otherwise, we have $\nu x.C = \nu\widetilde{y}.\langle Q\rangle\nu x.R$.

The LTS rules are given in Figure 2, with the exception of the symmetric rules (commuting P and Q) for LTS-PAR, LTS-FO, LTS-HO. The transitions are labeled with the (first-order or higher-order) names on which the communications may happen, or by τ for an internal evolution. The meta-variable α ranges over all the labels.

2.3 Barbed congruence

Behavioral equivalences may be defined either from the reduction or LTS semantics. We first give the definition of *barbed congruence*, which is a uniform definition of process equivalence among process calculi. It relies on the definition of *barbs*, i.e. the observable actions of a process. For HOπ, barbs are unrestricted first-order or higher-order names on which a communication may occur.

Definition 1. *For every first-order or higher-order name n, we define the strong observability predicates $P\downarrow_\mu$, with $\mu = n \mid \overline{n}$, as follows:*

- *We have $P\downarrow_{\overline{a}}$ iff $P \equiv \nu\widetilde{y}.(\overline{a}\langle Q\rangle R \mid S)$ with $a \notin \widetilde{y}$.*
- *We have $P\downarrow_{a}$ iff $P \equiv \nu\widetilde{y}.(a(X)Q \mid R)$ with $a \notin \widetilde{y}$.*
- *We have $P\downarrow_{\overline{m}}$ iff $P \equiv \nu\widetilde{y}.(\overline{m}.Q \mid R)$ with $m \notin \widetilde{y}$.*
- *We have $P\downarrow_{m}$ iff $P \equiv \nu\widetilde{y}.(m.Q \mid R)$ with $m \notin \widetilde{y}$.*

We now define barbed bisimulation on *closed processes*, i.e. processes with no free process variables. It relates processes with identical barbs that may keep this property by reduction.

Definition 2. *A relation $\mathcal{R}$ on closed process is a* strong barbed simulation *iff for all $(P, Q) \in\mathcal{R}$*

- *If $P\downarrow_\mu$ then $Q\downarrow_\mu$*
- *If $P \longrightarrow P'$, then there exists Q' such that $Q \longrightarrow Q'$ and $(P', Q') \in\mathcal{R}$.*

A relation $\mathcal{R}$ is a strong barbed bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are both strong barbed simulations. Two closed processes P and Q are* strongly barbed bisimilar*, iff there exists a strong barbed bisimulation $\mathcal{R}$ such that $(P, Q) \in\mathcal{R}$.*

We close the strong barbed bisimulation under contexts to define barbed congruence. As usual, contexts are terms with a hole; filling a context $\mathbb{C}$ with a process P gives a process written $\mathbb{C}\{P\}$. The grammar of HOπ contexts is:

$$\mathbb{C} ::= \square \mid \mathbb{C} \mid P \mid P \mid \mathbb{C} \mid \nu x.\mathbb{C} \mid \overline{a}\langle\mathbb{C}\rangle P \mid \overline{a}\langle P\rangle\mathbb{C} \mid a(X)\mathbb{C} \mid l.\mathbb{C} \mid !\mathbb{C}$$

In the following, we distinguish a subset of contexts called *evaluation contexts* $\mathbb{E}$:

$$\mathbb{E} ::= \square \mid \nu x.\mathbb{E} \mid \mathbb{E} \mid P \mid P \mid \mathbb{E}$$

Evaluation contexts are contexts which allow evolution (reduction) at the hole position: if $P \longrightarrow P'$, then we have $\mathbb{E}\{P\} \longrightarrow \mathbb{E}\{P'\}$.

Finally, barbed congruence is defined as:

Definition 3. *Closed processes P and Q are* strongly barbed congruent *iff $\mathbb{C}\{P\}$ and $\mathbb{C}\{Q\}$ are strongly barbed bisimilar for every context $\mathbb{C}$.*

Up to this point we have worked in the *strong* setting, where each reduction of P is matched by exactly one reduction of Q. In the *weak* case, a reduction of P may be matched by an arbitrary number (possibly zero) of reductions of Q. We write $\Longrightarrow$ the reflexive and transitive closure of $\longrightarrow$.

We define the weak observability predicate by $P \Downarrow_\mu$ iff there exists P' such that $P \Longrightarrow P' \downarrow_\mu$. We define barbed simulation by:

Definition 4. *A relation $\mathcal{R}$ on closed process is a* barbed simulation *iff for all $(P, Q) \in\mathcal{R}$*

- *If $P \downarrow_\mu$ then $Q \Downarrow_\mu$*
- *If $P \longrightarrow P'$, then there exists Q' such that $Q \Longrightarrow Q'$ and $(P', Q') \in\mathcal{R}$.*

A relation $\mathcal{R}$ is a barbed bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are both barbed simulations. Two closed processes P and Q are* barbed bisimilar*, iff there exists a barbed bisimulation $\mathcal{R}$ such that $(P, Q) \in\mathcal{R}$.*

Finally, we define barbed congruence:

Definition 5. *The closed processes P and Q are* barbed congruent*, iff $\mathbb{C}\{P\}$ and $\mathbb{C}\{Q\}$ are barbed bisimilar for every context $\mathbb{C}$.*

It is easy to prove that two processes are not barbed congruent: we just have to find a context $\mathbb{C}$ which distinguishes them. However, proving barbed congruence is more difficult because of the universal quantification on contexts. Consequently it is common in process calculi to find a simpler behavioral equivalence which characterizes barbed congruence.

2.4 Context bisimulation

Sangiorgi proposes *context* bisimulation as a LTS based alternative to barbed congruence. The definition of the (early strong) context bisimulation is:

Definition 6. *A relation $\mathcal{R}$ on closed processes is an early strong context simulation iff $P \mathcal{R} Q$ implies*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \mathcal{R} Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed concretions C, there exists G such that $Q \xrightarrow{a} G$ and $F \bullet C \mathcal{R} G \bullet C$.*
- *For all $P \xrightarrow{\overline{a}} C$, for all closed abstractions F, there exists D such that $Q \xrightarrow{\overline{a}} D$ and $F \bullet C \mathcal{R} F \bullet D$.*

A relation $\mathcal{R}$ is an early strong context bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are early strong context simulations. Two closed processes P and Q are strongly early context bisimilar, noted $P \mathrel{\mathcal{B}} Q$, iff there exists an early strong context bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

In the message sending and input cases, the context bisimulation introduces the surrounding environment which interacts with the processes P and Q. When sending a message (resp inputting a message), it considers all the abstractions F (resp concretions C) which may input (resp send) a message on the same channel a.

The relation is said to be *early* because the evolution G or D of Q depends on the choice of the interacting context. Another definition, where the two are independent, is said to be *late*.

Definition 7. *A relation $\mathcal{R}$ on closed processes is a late strong context simulation iff $P \mathrel{\mathcal{R}} Q$ implies*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{a} F$, there exists G such that $Q \xrightarrow{a} G$ and for all closed concretions C, we have $F \bullet C \mathrel{\mathcal{R}} G \bullet C$.*
- *For all $P \xrightarrow{\overline{a}} C$, there exists D such that $Q \xrightarrow{\overline{a}} D$ and for all closed abstractions F, we have $F \bullet C \mathrel{\mathcal{R}} F \bullet D$.*

A relation $\mathcal{R}$ is a late strong context bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are late strong context simulations. Two closed processes P and Q are strongly late context bisimilar iff there exists a late strong context bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

For HOπ, the early and late bisimilarities coincide [13], hence we can use both formulations. It is not the case in all calculi; for instance in the π-calculus, there exist early bisimilar processes which are not late bisimilar. In general the late version is easier to manipulate but is not *complete*, i.e. there exist processes which are barbed congruent but are not late bisimilar. On the other hand, early bisimulations are good candidates to characterize barbed congruence.

These definitions may be extended to the weak case. We note $\Rightarrow$ the reflexive and transitive closure of $\xrightarrow{\tau}$. In the definition of weak relations, a matching transition may include τ-action. A first possibility is to allow τ-actions before a visible action only: these relations are called *delay* bisimulations. For instance, the definition of the delay early context bisimulation is:

Definition 8. *A relation $\mathcal{R}$ on closed processes is a delay context simulation iff $P \mathrel{\mathcal{R}} Q$ implies*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \Rightarrow Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{l} P'$ with $l \neq \tau$, there exists Q' such that $Q \Rightarrow\xrightarrow{l} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*

- *For all* $P \xrightarrow{a} F$, *for all closed concretions* C, *there exists* G *such that* $Q \Rightarrow\xrightarrow{a} G$ *and* $F \bullet C \mathcal{R} G \bullet C$.
- *For all* $P \xrightarrow{\overline{a}} C$, *for all closed abstractions* F, *there exists* D *such that* $Q \Rightarrow\xrightarrow{\overline{a}} D$ *and* $F \bullet C \mathcal{R} F \bullet D$.

A relation $\mathcal{R}$ *is a delay context bisimulation iff* $\mathcal{R}$ *and* $\mathcal{R}^{-1}$ *are delay context simulations. Two closed processes* P *and* Q *are delay context bisimilar, iff there exists a delay context bisimulation* $\mathcal{R}$ *such that* $P \mathcal{R} Q$.

Delay bisimulations are generally easier to handle and some proof techniques may fail with non delay bisimulations (like for instance Howe's method given in Section 3.4). However delay bisimulations are generally not complete: there are processes which are weak barbed congruent but not delay context bisimilar. Another definition of weak relations is possible where τ-action are allowed before *and after* a visible action. We write $\overset{\tau}{\Rightarrow}$ for $\Rightarrow$. For all first-order name or coname n, we write $\overset{n}{\Rightarrow}$ for $\Rightarrow\xrightarrow{n}\Rightarrow$ and for all higher-order name or coname a, we write $\overset{a}{\Rightarrow}$ for $\Rightarrow\xrightarrow{a}$ (as higher order steps result in concretions and abstractions, they may not reduce further; silent steps after this reduction are taken into account in the definition of weak simulation below). We define weak early and late context bisimulations as:

Definition 9. *A relation* $\mathcal{R}$ *on closed processes is an early weak context simulation iff* $P \mathcal{R} Q$ *implies*

- *For all* $P \xrightarrow{l} P'$, *there exists* Q' *such that* $Q \overset{l}{\Rightarrow} Q'$ *and* $P' \mathcal{R} Q'$.
- *For all* $P \xrightarrow{a} F$, *for all closed concretions* C, *there exists* G, Q' *such that* $Q \overset{a}{\Rightarrow} G$, $G \bullet C \overset{\tau}{\Rightarrow} Q'$, *and* $F \bullet C \mathcal{R} Q'$.
- *For all* $P \xrightarrow{\overline{a}} C$, *for all closed abstractions* F, *there exists* D, Q' *such that* $Q \overset{\overline{a}}{\Rightarrow} D$, $F \bullet D \overset{\tau}{\Rightarrow} Q'$ *and* $F \bullet C \mathcal{R} Q'$.

A relation $\mathcal{R}$ *is an early weak context bisimulation iff* $\mathcal{R}$ *and* $\mathcal{R}^{-1}$ *are early weak context simulations. Two closed processes* P *and* Q *are early weak context bisimilar, iff there exists an early weak context bisimulation* $\mathcal{R}$ *such that* $P \mathcal{R} Q$.

Definition 10. *A relation* $\mathcal{R}$ *on closed processes is a late weak context simulation iff* $P \mathcal{R} Q$ *implies*

- *For all* $P \xrightarrow{l} P'$, *there exists* Q' *such that* $Q \overset{l}{\Rightarrow} Q'$ *and* $P' \mathcal{R} Q'$.
- *For all* $P \xrightarrow{a} F$, *there exists* G *such that* $Q \overset{a}{\Rightarrow} G$ *and for all closed concretions* C, *there exists* Q' *such that* $G \bullet C \overset{\tau}{\Rightarrow} Q'$ *and* $F \bullet C \mathcal{R} Q'$.
- *For all* $P \xrightarrow{\overline{a}} C$, *there exists* D *such that* $Q \overset{\overline{a}}{\Rightarrow} D$ *and for all closed abstractions* F, *there exists* Q' *such that* $F \bullet D \overset{\tau}{\Rightarrow} Q'$ *and* $F \bullet C \mathcal{R} F \bullet D$.

A relation $\mathcal{R}$ is a late weak context bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are late weak context simulations. Two closed processes P and Q are late weak context bisimilar iff there exists a late weak context bisimulation $\mathcal{R}$ such that $P \mathcal{R} Q$.

In the following, we use mainly the weak context definition, except when we explicitly refer to delay relations.

In the strong and weak cases, context bisimilarities are *sound*: two context bisimilar processes are barbed congruent. To prove this, Sangiorgi shows that context bisimilarities are *congruences*, i.e. if P and Q are context bisimilar, then $op(P)$ and $op(Q)$ are context bisimilar for all the operators op of the language. As a corollary, we deduce that if P and Q are context bisimilar, then for all contexts $\mathbb{C}$, $\mathbb{C}\{P\}$ and $\mathbb{C}\{Q\}$ are context bisimilar. As bisimilar processes have identical barbs, P and Q are barbed congruent.

To prove this congruence result on context bisimilarities, one relies on a *substitution lemma*:

Lemma 1. *Let A be an agent and P, Q be processes; if P and Q are strong (resp weak) context bisimilar, then $A\{P/X\}$ and $A\{Q/X\}$ are strong (resp weak) context bisimilar.*

The scheme of [13] to prove this lemma can be summed up by:

- The result is proved for evaluation contexts (parallel composition, replication, and restriction).
- The result is proved for all processes, using the first step.

The distinction is useful since if A is an evaluation context, the reductions of $A\{P/X\}$ may come from A or P, whereas if A is not an evaluation context, P cannot be reduced.

Context bisimulation is easy to understand: when two tested processes P and Q may perform a partial action (sending or receiving a message), it considers all the complementary contexts which may interact with P and Q. It is easier to manipulate than barbed congruence, since it features only one test in the internal action case. However, the universal quantification on concretions or abstractions makes the definition still hard to handle in practice. In the following, we give the definition of a simpler behavioral equivalence for HOπ.

2.5 Normal bisimulation

Normal bisimulation is a behavioral equivalence easier to use since it does not feature any universal quantification in its definition. It relies on an encoding of HOπ in a first-order π-calculus. Indeed, when we receive a process, we can only run, duplicate, discard, or forward it. These behaviors can be simulated by sending a name which is used as a trigger to run the process when needed. Formally, we have the following theorem (called *factorization theorem*):

Theorem 1. *For all A, Q, and m with $m \notin fn(A, Q)$, the agents $A\{Q/X\}$ and $\nu m.(A\{\overline{m}.\mathbf{0}/X\} \mid !m.Q)$ are weakly late context bisimilar.*

The factorization theorem allows to replace several copies of a process Q by a trigger $\overline{m}.\mathbf{0}$, which may activate a copy of Q when needed with the associated process $!m.Q$. Normal bisimulation relies on this translation to test weak equivalences of processes.

Definition 11. *A relation $\mathcal{R}$ on closed processes is a normal simulation iff $P \mathrel{\mathcal{R}} Q$ implies*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \overset{l}{\Rightarrow} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{a} (X)P'$, there exists $(X)Q'$ such that $Q \overset{a}{\Rightarrow} (X)Q'$ and for some $\overline{m}.\mathbf{0}$ where m is a fresh name, we have $P'\{\overline{m}.\mathbf{0}/X\} \mathrel{\mathcal{R}} Q'\{\overline{m}.\mathbf{0}/X\}$.*
- *For all $P \xrightarrow{\overline{a}} \nu\widetilde{x}.\langle R\rangle S$, there exists $\nu\widetilde{x'}.\langle R'\rangle S'$ such that $Q \overset{\overline{a}}{\Rightarrow} \nu\widetilde{x'}.\langle R'\rangle S'$ and for some fresh name m, we have $\nu\widetilde{x}.(S \mid !m.R) \mathrel{\mathcal{R}} \nu\widetilde{x'}.(S' \mid !m.R')$.*

A relation $\mathcal{R}$ is a normal bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are normal simulations. Two closed processes P and Q are normal bisimilar iff there exists a normal bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

In the message input case, normal bisimilarity tests only a trigger. In the message sending case, normal bisimilarity tests processes where the emitted processes R, R' are made available through a name m. Using the factorization theorem and the fact that weak late context bisimulation is a congruence, Sangiorgi proved that normal bisimilarity coincide with weak late context bisimilarity. Cao [2] extended the result to the strong case.

As we saw in this section, context bisimulation is a first step in finding a simple behavioral equivalence: it reduces only slightly the quantifications. On the other hand, normal bisimulation is a major improvement since only one test is perform at each transition step. We now study such relations for more expressive calculi.

3 Bisimulations in calculi with passivation

We now study bisimulations in calculi with passivation capabilities as in Homer or the Kell-calculus. Instead of working in Homer or Kell-calculus directly, we define a simpler calculus called HOπ with Passivation (HOπP), which extends HOπ with a passivation operator. By doing this we avoid the unnecessary features of Homer and Kell (mainly additional control on communication) and we are able to compare bisimulations in HOπ and HOπP.

$$P_1 \mid (P_2 \mid P_3) \equiv (P_1 \mid P_2) \mid P_3 \quad \textsc{Cong-Par-Assoc}$$

$$P_1 \mid P_2 \equiv P_2 \mid P_1 \quad \textsc{Cong-Par-Commut} \qquad P \mid \mathbf{0} \equiv P \quad \textsc{Cong-Par-Zero}$$

$$\nu x.\nu y.P \equiv \nu y.\nu x.P \quad \textsc{Cong-Restr-Commut}$$

$$\nu x.\mathbf{0} \equiv \mathbf{0} \quad \textsc{Cong-Restr-Zero} \qquad !P \equiv P \mid !P \quad \textsc{Cong-Replic}$$

$$\frac{x \notin \mathrm{fn}(P_1)}{\nu x.(P_1 \mid P_2) \equiv P_1 \mid \nu x.P_2} \quad \textsc{Cong-New-Par}$$

$$\frac{P \equiv Q}{\mathbb{C}\{P\} \equiv \mathbb{C}\{Q\}} \quad \textsc{Cong-Context}$$

Figure 3: Structural congruence for HOπP

3.1 Syntax and semantics of HOπP

We add localities $a[P]$, that are passivation units, to the HOπ constructs. With the same notations as for HOπ, the HOπP syntax is:

$$P ::= \mathbf{0} \;\mid\; X \;\mid\; P \mid P \;\mid\; l.P \;\mid\; a(X)P \;\mid\; \overline{a}\langle P\rangle P \;\mid\; \nu x.P \;\mid\; !P \;\mid\; a[P]$$

When passivation is not triggered, a locality $a[P]$ is a transparent evaluation context: process P may evolve by itself and communicate freely with processes outside of locality a. At any time, passivation may be triggered and the process $a[P]$ becomes a concretion $\langle P\rangle\mathbf{0}$. Passivation may thus occur as an internal τ step only if there is a receiver on a ready to receive the contents of the locality.

We extend localities to all agents: if $F = (X)P$, then $a[F] \triangleq (X)a[P]$; if $C = \nu\widetilde{x}.\langle Q\rangle R$, then $a[C] \triangleq \nu\widetilde{x}.\langle Q\rangle a[R]$. We also add the following rules to the LTS:

$$\frac{P \xrightarrow{\alpha} A}{a[P] \xrightarrow{\alpha} a[A]} \quad \text{LTS-}\textsc{Loc} \qquad\qquad a[P] \xrightarrow{\overline{a}} \langle P\rangle\mathbf{0} \quad \text{LTS-}\textsc{Passiv}$$

The reduction relation $\longrightarrow$ is defined as $\equiv\xrightarrow{\tau}\equiv$. The structural congruence relation $\equiv$ is the smallest equivalence relation that verifies the rules in Figure 3. Note that rule LTS-Loc implies that the scope of restricted names may cross locality boundaries. Scope extrusion outside localities is performed "by need" when a communication takes place. The reduction semantics, however, does not allow the restriction and locality operators to commute freely by structural congruence. If it did, there would be structurally congruent processes with different behavior. For instance, let $Q = a[\nu n.P] \mid a(X)(X \mid X)$. It reduces to $(\nu n.P) \mid (\nu n.P)$ by triggering the passivation. If we allow the structural extrusion of νn across locality a, we would have $Q \equiv \nu n.(a[P] \mid a(X)(X \mid X))$, which evolves to $\nu n.(P \mid P)$. In this case, the name n is shared by the two instances of P, whereas each instance of P has its own name n in the first case: the two obtained processes may have different reductions. For example, let $P = \overline{n}.\mathbf{0} \mid n.n.R$:

- In the first case, we have $(\nu n.(\overline{n}.\mathbf{0} \mid n.n.R)) \mid (\nu n.(\overline{n}.\mathbf{0} \mid n.n.R))$, which evolves in $(\nu n.n.R) \mid (\nu n.n.R)$. No further reduction is possible.
- In the second case, we get $\nu n.(\overline{n}.\mathbf{0} \mid \overline{n}.\mathbf{0} \mid n.n.R \mid n.n.R)$, which may evolve in $\nu n.(R \mid n.n.R)$. All the reductions of R are possible.

We now define HOπP contexts $\mathbb{C}$, evolution contexts $\mathbb{G}$, and evaluation contexts $\mathbb{E}$.

$$\mathbb{C} ::= \square \;\mid\; \mathbb{C} \mid P \;\mid\; P \mid \mathbb{C} \;\mid\; \nu x.\mathbb{C} \;\mid\; \overline{a}\langle\mathbb{C}\rangle P \;\mid\; \overline{a}\langle P\rangle\mathbb{C} \;\mid\; a(X)\mathbb{C} \;\mid\; l.\mathbb{C} \;\mid\; !\mathbb{C} \;\mid\; a[\mathbb{C}]$$

$$\mathbb{G} ::= \square \;\mid\; \nu x.\mathbb{G} \;\mid\; \mathbb{G} \mid P \;\mid\; P \mid \mathbb{G} \;\mid\; a[\mathbb{G}] \;\mid\; !\mathbb{G}$$

$$\mathbb{E} ::= \square \;\mid\; \nu x.\mathbb{E} \;\mid\; \mathbb{E} \mid P \;\mid\; P \mid \mathbb{E} \;\mid\; a[\mathbb{E}]$$

HOπP contexts simply extend the HOπ ones with the locality construct.

3.2 Characterization of barbed congruence

As in HOπ, our goal is to find a simple bisimulation-based characterization of barbed congruence. The definition of strong barbed congruence for HOπP is identical to Definition 3 after adapting the observability predicate. We note $P \sim_b Q$ to indicate that processes P and Q are strongly barbed congruent.

Definition 12. *For all first-order or higher-order name n, we define the strong observability predicates $P \downarrow_\mu$, with $\mu = n \mid \overline{n}$, as follows:*

- *We have $P \downarrow_{\overline{a}}$ iff $P = \mathbb{G}\{\overline{a}\langle Q\rangle R\}$ or $P = \mathbb{G}\{a[Q]\}$, with $a \notin bn(\mathbb{G})$.*
- *We have $P \downarrow_a$ iff $P = \mathbb{G}\{a(X)Q\}$ with $a \notin bn(\mathbb{G})$.*
- *We have $P \downarrow_{\overline{m}}$ iff $P = \mathbb{G}\{\overline{m}.Q\}$ with $m \notin bn(\mathbb{G})$.*
- *We have $P \downarrow_m$ iff $P = \mathbb{G}\{m.Q\}$ with $m \notin bn(\mathbb{G})$.*

Bound names of a context $\mathrm{bn}(\mathbb{C})$ are first-order and higher-order restricted names in $\mathbb{C}$ of whose scope encompasses the hole. For instance, a name $x \in \mathrm{fn}(P) \cap \mathrm{bn}(\mathbb{C})$ is free in P and becomes bound in $\mathbb{C}\{P\}$.

We now define a sound and complete context bisimulation for HOπP in the strong case. We first notice that the context bisimulation $\mathcal{B}$ given by Sangiorgi for HOπ (definition 6) is not sound in our calculus because of passivation. Bisimulation $\mathcal{B}$ relates the processes

$$P_0 = \overline{a}\langle\mathbf{0}\rangle !m.\mathbf{0} \qquad Q_0 = \overline{a}\langle m.\mathbf{0}\rangle !m.\mathbf{0}$$

The differences between the emitted processes $\mathbf{0}$ and $m.\mathbf{0}$ are shadowed by the process $!m.\mathbf{0}$. More precisely, we have to check that for all F, we have $F \bullet \langle \mathbf{0} \rangle !m.\mathbf{0} \;\mathcal{B}\; F \bullet \langle m.\mathbf{0} \rangle !m.\mathbf{0}$, i.e. for all R, we have $P' = R\{\mathbf{0}/X\} \;|!m.\mathbf{0} \;\mathcal{B}\; R\{m.\mathbf{0}/X\} \;|!m.\mathbf{0} = Q'$. We have three kinds of possible transitions from P':

- Transitions from R alone: they are matched by the same transitions of R in Q'
- Synchronisations between $!m.\mathbf{0}$ and R or $\xrightarrow{m}$-transitions from $!m.\mathbf{0}$: they are matched by the same transitions in Q'
- Synchronisations between the copies of the message $m.\mathbf{0}$ and R or $\xrightarrow{m}$-transitions from the message: they are matched by synchronizations between $!m.\mathbf{0}$ and R or $\xrightarrow{m}$-transitions from $!m.\mathbf{0}$ in Q'.

Conversely the transitions of Q' are matched by P'.

Remark 2. *This result can be proven formally by considering the relation* $\{(P\sigma \;|!m.\mathbf{0}, P\{\widetilde{\mathbf{0}}/\widetilde{X}\} \;|!m.\mathbf{0}), fv(P) \subseteq \widetilde{X}\}$, *where* σ *stands for a substitution which replaces some process variables with* $m.\mathbf{0}$ *and the others with* $\mathbf{0}$, *and showing that this relation is an early strong bisimulation according to definition 6.*

However P_0 and Q_0 are not barbed congruent in HOπP. The context $\mathbb{C} = b[\square] \mid a(X)X \mid b(X)\mathbf{0}$ distinguishes them. We have $\mathbb{C}\{P_0\} \longrightarrow b[!m.\mathbf{0}] \mid \mathbf{0} \mid b(X)\mathbf{0} = P'$ by a communication on a. This reduction is matched by $\mathbb{C}\{Q_0\} \longrightarrow b[!m.\mathbf{0}] \mid m.\mathbf{0} \mid b(X)\mathbf{0} = Q'$. By triggering the passivation on b, we have $P' \longrightarrow \mathbf{0}$ and $Q' \longrightarrow m.\mathbf{0}$. The two resulting processes are not barbed bisimilar.

In a message sending $\nu\widetilde{x}.\langle R \rangle S$, the emitted process R may be sent outside a passivation unit while the continuation S stays in this unit. If the passivation is triggered, the process S may be put in a different context, or may be destroyed (as shown in the previous example). Hence the passivation may separate the processes R and S and put them in totally different contexts, which is not possible in a calculus without passivation: the definition of the bisimulation has to be modified to take this into account.

The easiest way to adapt the bisimulation definition is to check in the concretion case that processes are still bisimilar when they are put in a locality. It means that we add the following condition (in the early case): if $P \xrightarrow{\overline{a}} C$, for all abstraction F, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $F \bullet a[C] \;\mathcal{R}\; F \bullet a[C']$. One of the possible evolutions of $F \bullet a[C]$ is triggering of the passivation and sending the contents of the locality (i.e. the continuation) in an arbitrary context. Consequently, the condition implies that for all evaluation context $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \;\mathcal{R}\; F \bullet \mathbb{E}\{C'\}$. Actually this new condition is enough to have a sound bisimulation. Therefore the definition of an early strong context bisimulation becomes:

Definition 13. *A relation* $\mathcal{R}$ *on closed processes is an early strong context simulation iff* $P \;\mathcal{R}\; Q$ *implies* $fn(P) = fn(Q)$ *and:*

- *For all* $P \xrightarrow{l} P'$*, there exists* Q' *such that* $Q \xrightarrow{l} Q'$ *and* $P' \mathcal{R} Q'$*.*
- *For all* $P \xrightarrow{a} F$*, for all closed concretions* C*, there exists* G *such that* $Q \xrightarrow{a} G$ *and* $F \bullet C \mathcal{R} G \bullet C$*.*
- *For all* $P \xrightarrow{\overline{a}} C$*, for all closed abstractions* F*, there exists* D *such that* $Q \xrightarrow{\overline{a}} D$ *and for all closed evaluation contexts* $\mathbb{E}$*, we have* $F \bullet \mathbb{E}\{C\} \mathcal{R} F \bullet \mathbb{E}\{D\}$*.*

A relation $\mathcal{R}$ *is an early strong context bisimulation iff* $\mathcal{R}$ *and* $\mathcal{R}^{-1}$ *are early strong context simulations. Two closed processes* P *and* Q *are early strongly context bisimilar, noted* $P \sim Q$*, iff there exists an early strong context bisimulation* $\mathcal{R}$ *such that* $P \mathcal{R} Q$*.*

This definition is similar to the ones for context bisimilarities in Homer [8] and the Kell-calculus [16] (except that in Kell, contexts are also added in the abstraction case).

Remark 3. *In the definition, the condition* $\mathit{fn}(P) = \mathit{fn}(Q)$ *has been added because of the lazy scope extrusion: two bisimilar processes with different free names may be distinguished because of this mechanism. For instance, a process* P *bisimilar to* $\mathbf{0}$ *but with a free name* y *(e.g.* $\nu x.x.y.\mathbf{0}$*) may be distinguished from* $\mathbf{0}$ *by a context* $\mathbb{C} = a[\nu y.\bar{b}\langle\Box\rangle R] \mid b(X)a(Y)(Y \mid Y)$*. The process* $\mathbb{C}\{P\}$ *may reduce to* $\nu y.(R \mid R)$*, while the process* $\mathbb{C}\{\mathbf{0}\}$ *evolves toward* $(\nu y.R) \mid (\nu y.R)$*. With an appropriate* R*, the two processes have different transitions, as illustrated in the discussion on commutation of name restriction and localities in Section 3.1. See the completeness proof in Appendix C for full details.*

The corresponding late version of context bisimulation is:

Definition 14. *A relation* $\mathcal{R}$ *on closed processes is a late strong context simulation iff* $P \mathcal{R} Q$ *implies* $\mathit{fn}(P) = \mathit{fn}(Q)$ *and:*

- *For all* $P \xrightarrow{l} P'$*, there exists* Q' *such that* $Q \xrightarrow{l} Q'$ *and* $P' \mathcal{R} Q'$*.*
- *For all* $P \xrightarrow{a} F$*, there exists* G *such that* $Q \xrightarrow{a} G$ *and for all closed concretions* C*, we have* $F \bullet C \mathcal{R} G \bullet C$*.*
- *For all* $P \xrightarrow{\overline{a}} C$*, there exists* D *such that* $Q \xrightarrow{\overline{a}} D$ *and for all closed abstractions* F *and evaluation contexts* $\mathbb{E}$*, we have* $F \bullet \mathbb{E}\{C\} \mathcal{R} F \bullet \mathbb{E}\{D\}$*.*

A relation $\mathcal{R}$ *is a late strong context bisimulation iff* $\mathcal{R}$ *and* $\mathcal{R}^{-1}$ *are late strong contxt simulations. Two closed processes* P *and* Q *are late strongly context bisimilar, noted* $P \sim_l Q$*, iff there exists a late strong context bisimulation* $\mathcal{R}$ *such that* $P \mathcal{R} Q$*.*

Both early and late strong bisimilarities are sound with respect to barbed congruence. This is given by the following theorem, whose proof can be found in Appendix A.

Theorem 2. *For all P, Q, if $P \sim Q$, or $P \sim_l Q$, then $P \sim_b Q$.*

In the following subsection, we discuss techniques, developed for the Kell-calculus and for Homer respectively, that can be used to show that context bisimulation is sound and complete in the strong case. We also explain why these techniques fail in the weak case, which remains an open problem.

3.3 Kell-calculus soundness proof

As in HOπ, the soundness proof used for the Kell-calculus relies on the substitution lemma (Lemma 1). However Sangiorgi's method to prove it (distinguishing between evaluation and other contexts) does not work in HOπP. Unlike HOπ, an execution context in HOπP may become a non-execution context (a locality may become a message output preventing internal reductions).

In concrete terms, to show the first step of Sangiorgi's method in the locality case, we would have to prove that if $P \sim Q$, then $a[P] \sim a[Q]$. We would have to build a relation $\mathcal{R}$ such that (with $P \sim Q$):

$$\begin{tikzcd}
a[P] \arrow[r, dash, dashed, "\mathcal{R}"] \arrow[d, "\tau"] & a[Q] \arrow[d, "\tau"] \\
\overline{a}\langle P\rangle\mathbf{0} \arrow[r, dash, dashed, "\mathcal{R}"] \arrow[d, "\overline{a}"] & \overline{a}\langle Q\rangle\mathbf{0} \arrow[d, "\overline{a}"] \\
\langle P\rangle\mathbf{0} \arrow[r, dash, dashed, "\mathcal{R}"] & \langle Q\rangle\mathbf{0}
\end{tikzcd}$$

and such that $\mathcal{R}$ is a bisimulation. Therefore for all abstractions $(X)R$, we would have $R\{P/X\} \; \mathcal{R} \; R\{Q/X\}$. To prove a sub-case of the substitution lemma, we would have to consider the relation $\mathcal{R}= \{(R\{P/X\}, R\{Q/X\}), P \sim Q\}$ and show that it is a bisimulation. But this would be the same as proving the substitution lemma directly. Hence Sangiorgi's proof method cannot be applied to HOπP.

The method used for the Kell-calculus is the following one. We define a relation $\mathcal{R} = \{(\mathbb{C}\{P\{\widetilde{R}/\widetilde{Y}\}\}, \mathbb{C}\{P\{\widetilde{S}/\widetilde{Y}\}\}), \mathrm{fv}(P) = \widetilde{Y}, \widetilde{R} \sim \widetilde{S}\}$, and we show that its reflexive and transitive closure is an early or late bisimulation. We suppose now that we work with the early definition, but the proof technique work with the late one as well.

We first explain why we work with the reflexive and transitive closure instead of the relation itself. To show that $\mathcal{R}$ is a bisimulation, we proceed by induction on the derivation of the transition $P\{\widetilde{R}/\widetilde{Y}\} \xrightarrow{\alpha} P'$ (in the case $\mathbb{C} = \square$). Consider the case of the parallel composition $P = Q \mid T$, and we suppose that P evolves by a higher-order communication. We want to close the following diagram:

$$\begin{tikzcd}
Q_R \mid T_R \arrow[r, dash, "\mathcal{R}"] \arrow[d, "\tau"] & Q_S \mid T_S \\
F_R \bullet C_R &
\end{tikzcd}$$

knowing that $Q_R \xrightarrow{a} F_R$ and $T_R \xrightarrow{\overline{a}} C_R$ for some a (for all processes $P, \widetilde{R}$, we write P_R for $P\{\widetilde{R}/\widetilde{Y}\}$. We have $Q_R \mathrel{\mathcal{R}} Q_S$ so by applying C_R to F_R (we work with early bisimulation, hence we have to choose the concretion before getting a matching abstraction), we have by induction:

$$\begin{tikzcd}
Q_R \arrow[r, dash, "\mathcal{R}"] \arrow[d, "a"] & Q_S \arrow[d, dashed, "a"] \\
F_R \arrow[r, dash, dashed, "\mathcal{R}"] & F_S
\end{tikzcd}$$

with $F_R \bullet C_R \mathrel{\mathcal{R}} F_S \bullet C_R$.

We have $T_R \mathrel{\mathcal{R}} T_S$, so by applying C_R to F_S we have:

$$\begin{tikzcd}
T_R \arrow[r, dash, "\mathcal{R}"] \arrow[d, "\overline{a}"] & T_S \arrow[d, dashed, "\overline{a}"] \\
C_R \arrow[r, dash, dashed, "\mathcal{R}"] & C_S
\end{tikzcd}$$

with $F_S \bullet C_R \mathrel{\mathcal{R}} F_S \bullet C_S$. From these we can conclude that:

$$\begin{tikzcd}
Q_R \mid T_R \arrow[rr, dash, "\mathcal{R}"] \arrow[d, "\tau"'] & & Q_S \mid T_S \arrow[d, dashed, "\tau"] \\
F_R \bullet C_R \arrow[r, dash, dashed, "\mathcal{R}"] & F_S \bullet C_R \arrow[r, dash, dashed, "\mathcal{R}"] & F_S \bullet C_S
\end{tikzcd}$$

As a result, we have:

$$\begin{tikzcd}
P_R \arrow[r, dash, "\mathcal{R}"] \arrow[d, "\tau"] & P_S \arrow[d, dashed] \\
P'_R \arrow[r, dash, dashed, "\mathcal{R}^2"] & P'_S
\end{tikzcd}$$

while we need $P'_R \mathrel{\mathcal{R}} P'_S$.

More generally, we prove that $\mathcal{R}$ *progresses* towards its reflexive and transitive closure $\mathcal{R}^*$, i.e. if $(P, Q) \in \mathcal{R}$ and $P \xrightarrow{a} P'$, then there exists Q' such that $Q \xrightarrow{a} Q'$ and $(P', Q') \in \mathcal{R}^*$ (see appendix D for details).

$$\begin{tikzcd}
P \arrow[r, dash, "\mathcal{R}"] \arrow[d, "a"] & Q \arrow[d, dashed, "a"] \\
P' \arrow[r, dash, dashed, "\mathcal{R}^*"] & Q'
\end{tikzcd}$$

In the strong case, it is sufficient to show that $\mathcal{R}^*$ is a bisimulation. Suppose that $P\ \mathcal{R}^*\ Q$ and $P \xrightarrow{a} P'$. There exists $P_1, \dots, P_n$ such that $P\ \mathcal{R}\ P_1\ \mathcal{R} \dots P_n\ \mathcal{R}\ Q$. We want to close the following diagram:

$$\begin{tikzcd} P \arrow[r, dash, "\mathcal{R}"] \arrow[d, "a"] & P_1 \arrow[r, dotted, dash] & P_n \arrow[r, dash, "\mathcal{R}"] & Q \\ P' & & & \end{tikzcd}$$

Since $\mathcal{R}$ progress towards $\mathcal{R}^*$, we build $P_1' \dots P_n', Q'$ such that $P'\ \mathcal{R}^*\ P_1'\ \mathcal{R}^* \dots P_n'\ \mathcal{R}^*\ Q'$.

$$\begin{tikzcd} P \arrow[r, dash, "\mathcal{R}"] \arrow[d, "a"] & P_1 \arrow[r, dotted, dash] \arrow[d, dashed, "a"] & P_n \arrow[r, dash, "\mathcal{R}"] \arrow[d, dashed, "a"] & Q \arrow[d, dashed, "a"] \\ P' \arrow[r, dashed, dash, "\mathcal{R}^*"] & P_1' \arrow[r, dotted, dash] & P_n' \arrow[r, dashed, dash, "\mathcal{R}^*"] & Q' \end{tikzcd}$$

Since $\mathcal{R}^*$ is transitive, we have $P'\ \mathcal{R}^*\ Q'$ as required. The soundness proof using the Kell-calculus technique can be found in Appendix A.

This approach fails in the weak case. We want to close the following diagram:

$$\begin{tikzcd} P \arrow[r, dash, "\mathcal{R}"] \arrow[d, "a"] & P_1 \arrow[r, dotted, dash] & P_n \arrow[r, dash, "\mathcal{R}"] & Q \\ P' & & & \end{tikzcd}$$

We use the fact that $\mathcal{R}$ progress towards $\mathcal{R}^*$ for P, P', P_1.

$$\begin{tikzcd} P \arrow[r, dash, "\mathcal{R}"] \arrow[ddd, "a"] & P_1 \arrow[r, dash, "\mathcal{R}"] \arrow[d, dashed, "\tau"] & P_2 \arrow[r, dotted, dash] & P_n \arrow[r, dash, "\mathcal{R}"] & Q \\ & P_{12} \arrow[d, dashed, "\tau"] & & & \\ & P_{13} \arrow[d, Rightarrow, dashed, "a"] & & & \\ P' \arrow[r, dashed, dash, "\mathcal{R}^*"] & P_1' & & & \end{tikzcd}$$

We close the sub-diagram P_1, P_{12}, P_2:

$$X \mathrel{\widehat{\mathcal{R}}} X \qquad \mathbf{0} \mathrel{\widehat{\mathcal{R}}} \mathbf{0} \qquad \frac{P \mathrel{\mathcal{R}} Q}{l.P \mathrel{\widehat{\mathcal{R}}} l.Q} \qquad \frac{P \mathrel{\mathcal{R}} Q}{\nu x.P \mathrel{\widehat{\mathcal{R}}} \nu x.Q} \qquad \frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{P_1 \mid P_2 \mathrel{\widehat{\mathcal{R}}} Q_1 \mid Q_2}$$

$$\frac{P \mathrel{\mathcal{R}} Q}{a(X)P \mathrel{\widehat{\mathcal{R}}} a(X)Q} \qquad \frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{\overline{a}\langle P_1 \rangle P_2 \mathrel{\widehat{\mathcal{R}}} \overline{a}\langle Q_1 \rangle Q_2} \qquad \frac{P \mathrel{\mathcal{R}} Q}{!P \mathrel{\widehat{\mathcal{R}}} !Q} \qquad \frac{P \mathrel{\mathcal{R}} Q}{a[P] \mathrel{\widehat{\mathcal{R}}} a[Q]}$$

Figure 4: Compatible refinement for HOπP

$$\begin{tikzcd}
P \arrow[r, dash, "\mathcal{R}"] \arrow[ddd, "a"'] & P_1 \arrow[r, dash, "\mathcal{R}"] \arrow[d, dashed, "\tau"] & P_2 \arrow[r, dotted, dash] \arrow[d, Rightarrow, dashed] & P_n \arrow[r, dash, "\mathcal{R}"] & Q \\
& P_{12} \arrow[r, dashed, dash, "\mathcal{R}^*"] \arrow[d, dashed, "\tau"] & P_{22} & & \\
& P_{13} \arrow[d, Rightarrow, dashed, "a"] & & & \\
P' \arrow[r, dashed, dash, "\mathcal{R}^*"] & P_1' & & &
\end{tikzcd}$$

Hence we have $P_{12} \mathrel{\mathcal{R}^*} P_{22}$ and $P_{12} \xrightarrow{\tau} P_{13}$: the diagram P, Q, P' we want to close may be smaller than P_{12}, P_{22}, P_{13}. The scheme may then recursively and infinitely repeat itself. Knowing that $\mathcal{R}$ progress towards $\mathcal{R}^*$ does not allow to prove that $\mathcal{R}^*$ is a bisimulation in the weak case. This problem is similar to the application of up-to techniques in the weak case [14]. Hence we cannot show that the early bisimulation is a congruence in the weak case with this technique.

Remark 4. *We have the same results with the late bisimulation: we can prove that the late bisimulation is a congruence in the strong case, but the weak one remains an open problem.*

Remark 5. *On the contrary the method used by Sangiorgi may easily be adapted in the weak case for HOπ without passivation. Transitivity issues are dealt with by using up-to techniques mixing strong and weak bisimilarities. See [13] for further details.*

3.4 Howe's method and input-early bisimulations

Howe's method [1, 7] is a systematic proof technique to show that a candidate relation $\mathcal{R}$ is a congruence. It has been used for Homer to show first that late bisimilarity is sound [8], and has been adapted to show that *input early* bisimilarity is sound [6]. We introduce input-early bisimulations later; we first explain Howe's technique and its application to late bisimulations.

Instead of showing that $\mathcal{R}$ is a congruence directly, Howe's method builds a relation $\mathcal{R}^\bullet$ (the *Howe closure* of $\mathcal{R}$) which is immediately a congruence and which is very close to bisimulation by construction. Additional properties which relate $\mathcal{R}$ and $\mathcal{R}^\bullet$ allow to conclude that $\mathcal{R}$ is a congruence.

The definition of the Howe closure relies on auxiliary relations, the open extension of $\mathcal{R}$ noted $\mathcal{R}^\circ$ and the compatible refinement of $\mathcal{R}$, noted $\widehat{\mathcal{R}}$. The open extension extends the definition of the relation $\mathcal{R}$ to open processes, i.e. to processes with free process variables X:

Definition 15. *Let P and Q be two open processes. We have $P\ \mathcal{R}^\circ\ Q$ iff $P\sigma\ \mathcal{R}\ Q\sigma$ for all substitutions that close P and Q.*

The compatible refinement of a relation is inductively defined for HOπP by the rules given figure 4. These rules formalize the fact that two processes are related by $\widehat{\mathcal{R}}$ iff they have the same syntactic shape and if their immediate sub-processes are related by $\mathcal{R}$.

Definition 16. *The Howe's closure $\mathcal{R}^\bullet$ of a relation $\mathcal{R}$ is inductively defined by the following rule:*

$$\frac{P\ \widehat{\mathcal{R}^\bullet}\ Q \qquad Q\ \mathcal{R}^\circ\ R}{P\ \mathcal{R}^\bullet\ R}$$

The composition of the relations $\widehat{\mathcal{R}^\bullet}$ and $\mathcal{R}^\circ$ gives to the Howe closure congruence properties but allows also some transitivity. Indeed we have the following properties:

Lemma 2. *If $\mathcal{R}$ is an equivalence, then $\mathcal{R}^\bullet$ is reflexive and:*

$$\frac{P\ \widehat{\mathcal{R}^\bullet}\ Q}{P\ \mathcal{R}^\bullet\ Q}\ \textsc{Cong} \qquad \frac{P\ \mathcal{R}^\circ\ Q}{P\ \mathcal{R}^\bullet\ Q}\ \textsc{Open} \qquad \frac{P\ \mathcal{R}^\bullet\ P' \qquad P'\ \mathcal{R}^\circ\ Q}{P\ \mathcal{R}^\bullet\ Q}\ \textsc{Open right}$$

$$\frac{P\ \mathcal{R}^\bullet\ Q \qquad P'\ \mathcal{R}^\bullet\ Q'}{P\{P'/X\}\ \mathcal{R}^\bullet\ Q\{Q'/X\}}\ \textsc{Subst}$$

By rule Cong we know that the Howe closure is a congruence. Rule Open right allows a composition on the right, and rule Subst allows substitutions to take place inside two processes related by the Howe closure. These properties can be proved by induction or follow immediately from the definition and from the fact that $\mathcal{R}$ (and then $\mathcal{R}^\circ$) is an equivalence.

In our case we want to show that a bisimulation $\mathcal{B}$ is a congruence. Following the Howe's method scheme we have to prove that $\mathcal{B}^\bullet{=}\mathcal{B}^\circ$. Since $\mathcal{B}^\bullet$ is a congruence and $\mathcal{B}^\circ$ equals $\mathcal{B}$ on closed terms, we conclude that $\mathcal{B}$ is a congruence.

With Open, we already have $\mathcal{B}^\circ{\subseteq}\mathcal{B}^\bullet$. The reverse inclusion can be established by proving a modified simulation property for $\mathcal{B}^\bullet$. Proving that a congruence has some bisimulation properties raises some transitivity issues as pointed out with the previous technique, and consequently cannot be applied in the weak case. To deal with this issue, the modified bisimulation property has to feature some transitivity. It is easy for late bisimulation: we extend $\sim_l^\bullet$ to abstractions by $F \sim_l^\bullet F'$ iff for all C, we have $F \bullet C \sim_l^\bullet F' \bullet C$. We have then the following property:

Lemma 3. *If $P \sim_l^\bullet Q$, then:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \sim_l^\bullet Q'$.*
- *For all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and $F \sim_l^\bullet F'$*
- *For all $P \xrightarrow{\overline{a}} C$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all closed F, F' such that $F \sim_l^\bullet F'$ and all evaluation contexts $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \sim_l^\bullet F' \bullet \mathbb{E}\{C'\}$.*

The transitivity is built in the output clause of this bisimulation-like property: F and C are directly related to F' and C'. With this lemma and properties of Howe's closure, we can prove that $\sim_l$ is a congruence.

For late bisimilarities, it is possible to prove bisimulation-like properties featuring some transitivity for Howe's closure: we can work with abstractions and concretions independently. It is not case for early bisimilarities. However the method can be adapted to work with *input-early* bisimulations [6], which are bisimulations with an early condition in the input clause and a late condition in the output one. The definition is:

Definition 17. *A relation $\mathcal{R}$ on closed processes is an input-early strong simulation iff $P \mathcal{R} Q$ implies $fn(P) = fn(Q)$ and:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \mathcal{R} Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed concretions C and closed evaluation contexts $\mathbb{F}$, there exists G such that $Q \xrightarrow{a} G$ and $\mathbb{F}\{F\} \bullet C \mathcal{R} \mathbb{F}\{G\} \bullet C$.*
- *For all $P \xrightarrow{\overline{a}} C$, there exists D such that $Q \xrightarrow{\overline{a}} D$ and for all closed abstractions F and evaluation contexts $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \mathcal{R} F \bullet \mathbb{E}\{D\}$.*

A relation $\mathcal{R}$ is an input-early strong bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are input-early strong simulations. Two closed processes P and Q are input-early strongly bisimilar, noted $P \sim_{ie} Q$, iff there exists an input-early strong bisimulation $\mathcal{R}$ such that $P \mathcal{R} Q$.

Evaluation contexts have been added in the message input clause for technical reasons. Concretions remain independent from abstractions, so we extend $\sim_{ie}^\bullet$ to concretions:

$$\frac{P \sim_{ie}^\bullet P' \qquad Q \sim_{ie}^\bullet Q' \qquad \langle P'\rangle Q' \sim_{ie}^\circ C}{\langle P\rangle Q \sim_{ie}^\bullet C} \qquad\qquad \frac{C \sim_{ie}^\bullet D \qquad \nu x.D \sim_{ie}^\circ C'}{\nu x.C \sim_{ie}^\bullet C'}$$

with $C \sim_{ie}^{\circ} C'$ iff for all F, $F \bullet C \sim_{ie}^{\circ} F \bullet C'$. We extend $\sim_{ie}^{\bullet}$ by adding the rule $\square \sim_{ie}^{\bullet} \square$, and we show this bisimulation-like property for input-early Howe's closure:

Lemma 4. *Let $(\sim_{ie})_c^{\bullet}$ be the restriction of $\sim_{ie}^{\bullet}$ to closed terms. If $P\ (\sim_{ie})_c^{\bullet}\ Q$ then :*

- *If $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P'\ (\sim_{ie})_c^{\bullet}\ Q'$.*
- *If $P \xrightarrow{a} F$, for all closed concretion $C\ (\sim_{ie})_c^{\bullet}\ C'$ and evaluation contexts $\mathbb{E} \sim_{ie}^{\bullet} \mathbb{E}'$, there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}\{F\} \bullet C\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'\{F'\} \bullet C'$*
- *If $P \xrightarrow{\overline{a}} C$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all closed evaluation contexts $\mathbb{E}, \mathbb{E}'$ such that $\mathbb{E} \sim_{ie}^{\bullet} \mathbb{E}'$, we have $\mathbb{E}\{C\}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'\{C'\}$.*

The property features transitivity in the input clause. Using this lemma and properties of Howe's closure, we can prove that $\sim_{ie}^{\bullet}$ is a bisimulation and coincide with $\sim_{ie}$. The complete soundness proof of input-early strong bisimilarity using Howe's method can be found in appendix B. The proof can be extended to the late weak *delay* bisimulation. However it cannot be used for early bisimilarities.

Until now, we have proved that early context bisimulation is sound in the strong case, using the Kell-calculus method, and that input-early bisimulation is sound in the strong and weak cases using Howe's method. In the following section, we show that both relations are complete in the strong case.

3.5 Completeness

Early bisimulation and input-early are sound in the strong case. We prove that they are also complete. It means that the two relations coincide, and that we have a full characterization of the strong barbed congruence.

Theorem 3. *For all P, Q, if $P \sim_b Q$ then $P \sim Q$ and $P \sim_{ie} Q$.*

The theorem is proved by contradiction. We sketch the proof here. The detailed proof of completeness for both relations, $\sim$ and $\sim_{ie}$, can be found in Appendix C. We define two families of relations $\sim_k, \sim_{ie,k}$, with k an integer, which differentiate several levels of bisimulations by stating that processes have to be bisimilar only during the first k steps, and such that $\sim = \bigcap_k \sim_k$ and $\sim_{ie} = \bigcap_k \sim_{ie,k}$:

- The relations $\sim_0, \sim_{ie,0}$ relate the processes with the same free names, ie. $\sim_0 = \sim_{ie,0} = \{(P,Q), \mathrm{fn}(P) = \mathrm{fn}(Q)\}$
- We have $P \sim_k Q$ iff
  - For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \sim_{k-1} Q'$, and conversely for all $Q \xrightarrow{l} Q'$.

  - For all $P \xrightarrow{a} F$, for all closed concretion C, there exists G such that $Q \xrightarrow{a} G$ and $F \bullet C \sim_{k-1} G \bullet C$, and conversely for all $Q \xrightarrow{a} F$.
  - For all $P \xrightarrow{\overline{a}} C$, for all closed abstraction F, there exists D such that $Q \xrightarrow{\overline{a}} D$ and for all closed evaluation context $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \sim_{k-1} F \bullet \mathbb{E}\{D\}$, and conversely for all $Q \xrightarrow{\overline{a}} C$.

- We have $P \sim_{ie,k} Q$ iff
  - For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \sim_{ie,k-1} Q'$, and conversely for all $Q \xrightarrow{l} Q'$.
  - For all $P \xrightarrow{a} F$, for all closed concretions C and evaluation contexts $\mathbb{E}$, there exists G such that $Q \xrightarrow{a} G$ and $\mathbb{E}\{F\} \bullet C \sim_{ie,k-1} \mathbb{E}\{G\} \bullet C$, and conversely for all $Q \xrightarrow{a} F$.
  - For all $P \xrightarrow{\overline{a}} C$, there exists D such that $Q \xrightarrow{\overline{a}} D$ and for all closed abstractions F and closed evaluation contexts $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \sim_{ie,k-1} F \bullet \mathbb{E}\{D\}$, and conversely for all $Q \xrightarrow{\overline{a}} C$.

By induction we prove that if for some k we have $P \nsim_k Q$ or $P \nsim_{ie,k} Q$, then there exists a context $\mathbb{C}_k$ such that $\mathbb{C}_k\{P\} \nsim_b \mathbb{C}_k\{Q\}$. If $P \nsim Q$ (resp $P \nsim_{ie} Q$), then there exists k such that $P \nsim_k Q$ (resp $P \nsim_{ie,k} Q$), hence there exists a context $\mathbb{C}$ such that $\mathbb{C}\{P\} \nsim_b \mathbb{C}\{Q\}$. Consequently P and Q are not strongly barbed congruent.

3.6 Summary

The behavioral theory of HOπP is severely lacking, compared to the one of HOπ. In the strong case, early or input-early strong context bisimilarity characterizes strong barbed congruence. In the weak case, only sound relations (input-early or late context bisimilarities) have been found. Context bisimulations are more complex than in HOπ since they feature additional quantifications on contexts. Simplifications of these relations similar to normal bisimulations have yet to be found.

In the next section, we show that this additional complexity is due to the relationship between passivation and name restriction. We remove name restriction $\nu x.P$ from HOπP and we show that in this calculus with passivation but without restriction, called HOP, we can define a simpler context bisimulation and a normal bisimulation. We also present counter-examples that show that this approach does not work for HOπP.

4 HOP: Removing restriction from HOπP

In this section, we show that the behavioral theory of the calculus HOP is similar to the one of HOπ: we are able to define simple context and normal bisimilarities which characterize barbed congruence.

$$P \mid (Q \mid R) \equiv (P \mid Q) \mid R \quad \textsc{Cong-Par-Assoc}$$

$$P \mid Q \equiv Q \mid P \quad \textsc{Cong-Par-Commut} \qquad P \mid \mathbf{0} \equiv P \quad \textsc{Cong-Par-Zero}$$

$$!P \equiv P \mid !P \quad \textsc{Cong-Replic} \qquad P + Q \equiv Q + P \quad \textsc{Cong-Sum-Commut}$$

$$P + (Q + R) \equiv (P + Q) + R \quad \textsc{Cong-Sum-Assoc}$$

$$P + \mathbf{0} \equiv P \quad \textsc{Cong-Sum-Zero} \qquad \frac{P \equiv Q}{\mathbb{C}\{P\} \equiv \mathbb{C}\{Q\}} \quad \textsc{Cong-Context}$$

Figure 5: Structural congruence

4.1 Syntax and semantics

The syntax of the Light Higher-Order π-calculus with Passivation (HOP) is given below. Without restriction, it is no longer possible to compositionally encode choice (which is necessary to obtain a simple characterization of barbed congruence), so we add this operator to the calculus.

$$P ::= \mathbf{0} \;\mid\; X \;\mid\; P \mid P \;\mid\; l.P \;\mid\; a(X)P \;\mid\; \overline{a}\langle P\rangle P \;\mid\; a[P] \;\mid\; !P \;\mid\; P + P$$

The LTS semantics becomes simpler since we do not have to worry about scope extrusion: concretions are now simply written $\langle R\rangle S$. Pseudo-application $\bullet$ between an abstraction $F = (X)P$ and a concretion $C = \langle R\rangle Q$ becomes:

$$(X)P \bullet \langle R\rangle Q \triangleq P\{R/X\} \mid Q$$

However we have to give rules for the added choice operator. Rules of the LTS are given Figure 6, except symmetric rules for LTS-Par, LTS-FO, LTS-HO and LTS-Sum. The structural congruence rules can be found in Figure 5.

4.2 Barbed congruence and context bisimulations

We first modify the observability predicate, since name restriction may no longer hide observables. We also add replication and choice to evolution contexts. The syntax of HOP evolution contexts is:

$$\mathbb{G} ::= \Box \;\mid\; \mathbb{G} \mid P \;\mid\; P \mid \mathbb{G} \;\mid\; a[\mathbb{G}] \;\mid\; !\mathbb{G} \;\mid\; \mathbb{G} + P \;\mid\; P + \mathbb{G}$$

The definition of the strong observability predicate becomes:

Definition 18. *For all first-order or higher-order name n, we define the strong observability predicates $P \downarrow_\mu$, with $\mu = n \mid \overline{n}$, as follows:*

- *We have $P \downarrow_{\overline{a}}$ iff $P = \mathbb{G}\{\overline{a}\langle Q\rangle R\}$ or $P = \mathbb{G}\{a[Q]\}$.*

$$l.P \xrightarrow{l} P \quad \text{LTS-Prefix} \qquad a(X)P \xrightarrow{a} (X)P \quad \text{LTS-Abstr}$$

$$\overline{a}\langle Q\rangle P \xrightarrow{\overline{a}} \langle Q\rangle P \quad \text{LTS-Concr} \qquad \frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q} \quad \text{LTS-Par}$$

$$\frac{P \xrightarrow{\alpha} A}{P + Q \xrightarrow{\alpha} A} \quad \text{LTS-Sum} \qquad \frac{P \xrightarrow{\alpha} A}{!P \xrightarrow{a} A \mid !P} \quad \text{LTS-Replic}$$

$$\frac{P \xrightarrow{a} F \qquad P \xrightarrow{\overline{a}} C}{!P \xrightarrow{\tau} F \bullet C \mid !P} \quad \text{LTS-Replic-HO}$$

$$\frac{P \xrightarrow{m} P_1 \qquad P \xrightarrow{\overline{m}} P_2}{!P \xrightarrow{\tau} P_1 \mid P_2 \mid !P} \quad \text{LTS-Replic-FO}$$

$$\frac{P \xrightarrow{m} P' \qquad Q \xrightarrow{\overline{m}} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'} \quad \text{LTS-FO} \qquad \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \quad \text{LTS-HO}$$

$$\frac{P \xrightarrow{\alpha} A}{a[P] \xrightarrow{\alpha} a[A]} \quad \text{LTS-Loc} \qquad a[P] \xrightarrow{\overline{a}} \langle P\rangle\mathbf{0} \quad \text{LTS-Passiv}$$

Figure 6: HOP: Labelled transition system

- *We have* $P \downarrow_a$ *iff* $P = \mathbb{G}\{a(X)Q\}$.
- *We have* $P \downarrow_{\overline{m}}$ *iff* $P = \mathbb{G}\{\overline{m}.Q\}$.
- *We have* $P \downarrow_m$ *iff* $P = \mathbb{G}\{m.Q\}$.

Evaluation contexts $\mathbb{E}$ in HOP have the same form as those in HOπP. The definition of the strong barbed congruence is similar to Definition 3. We continue to write $P \sim_b Q$ to denote that processes P and Q are strong barbed congruent.

We now give a definition of bisimulation which characterizes barbed congruence. As pointed out in Section 3.2, in the concretion case passivation may put the message and its continuation in different contexts. However since name restriction has been removed, they may not share private channels. Instead of keeping message and continuation together, we can now study them separately and still have a complete bisimilarity. We propose the following bisimulation, similar to the higher-order bisimulation given by Thomsen for Plain CHOCS [17]. For an abstraction $F = (X)P$ and a process R, we write $F \circ R$ for $P\{R/X\}$.

Definition 19. *A relation $\mathcal{R}$ on closed processes is an early strong HO simulation iff $P \mathrel{\mathcal{R}} Q$ implies:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed processes R, there exists F' such that $Q \xrightarrow{a} F'$ and $F \circ R \mathrel{\mathcal{R}} F' \circ R$.*
- *For all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S' such that $Q \xrightarrow{\overline{a}} \langle R' \rangle S'$, $R \mathrel{\mathcal{R}} R'$, $S \mathrel{\mathcal{R}} S'$.*

A relation $\mathcal{R}$ is an early strong HO bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are early strong context simulations. Two closed processes P and Q are strongly early HO bisimilar, noted $P \dot{\sim} Q$, iff there exists an early strong HO bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

We notice that this HO bisimulation is easier to use than the context simulation for HOπP since a test on all processes is performed only in the abstraction case. This HO bisimulation is a characterization of barbed bisimulation. First, the relation is sound:

Theorem 4. *The early strong HO bisimilarity $\dot{\sim}$ is a congruence.*

For the proof, we use the Kell-calculus technique described earlier. See Appendix D for details.

The early strong HO bisimulation is also complete:

Theorem 5. *For all P, Q, if $P \sim_b Q$ then $P \dot{\sim} Q$.*

We use the same technique as for HOπP. The proof can be found in Appendix E.

In the following we also use the late counterpart of HO bisimulation, given below:

Definition 20. *A relation $\mathcal{R}$ on closed processes is a late strong HO simulation iff $P \mathrel{\mathcal{R}} Q$ implies:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and for all closed processes R, $F \circ R \mathrel{\mathcal{R}} F' \circ R$.*
- *For all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S' such that $Q \xrightarrow{\overline{a}} \langle R' \rangle S'$ and $R \mathrel{\mathcal{R}} R'$ and $S \mathrel{\mathcal{R}} S'$.*

A relation $\mathcal{R}$ is a late strong HO bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are late strong HO simulations. Two closed processes P and Q are strongly late HO bisimilar, noted $P \mathrel{\dot{\sim}_l} Q$, iff there exists a late strong HO bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

We show later that early and late HO bisimulations coincide. Consequently the (simpler) late formulation is also suitable to prove behavioral equivalence of processes.

These definitions and results may be extended to weak bisimulations. We define weak HO bisimulations as follows:

Definition 21. *A relation $\mathcal{R}$ on closed processes is an early weak HO simulation iff $P \mathrel{\mathcal{R}} Q$ implies:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \overset{l}{\Rightarrow} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed processes R, there exists F', Q' such that $Q \overset{a}{\Rightarrow} F'$, $F' \circ R \overset{\tau}{\Rightarrow} Q'$, and $F \circ R \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S'', S' such that $Q \overset{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \overset{\tau}{\Rightarrow} S'$, $R \mathrel{\mathcal{R}} R'$, and $S \mathrel{\mathcal{R}} S'$.*

A relation $\mathcal{R}$ is an early weak HO bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are early weak HO simulations. Two closed processes P and Q are weakly early HO bisimilar, noted $P \mathrel{\dot{\approx}} Q$, iff there exists an early weak HO bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

Definition 22. *A relation $\mathcal{R}$ on closed processes is a late weak HO simulation iff $P \mathrel{\mathcal{R}} Q$ implies:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \overset{l}{\Rightarrow} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{a} F$, there exists F' such that $Q \overset{a}{\Rightarrow} F'$ and for all closed processes R, there exists Q' such that $F' \circ R \overset{\tau}{\Rightarrow} Q'$ and $F \circ R \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S'', S' such that $Q \overset{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \overset{\tau}{\Rightarrow} S'$, $R \mathrel{\mathcal{R}} R'$, and $S \mathrel{\mathcal{R}} S'$.*

A relation $\mathcal{R}$ is a late weak HO bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are late weak context simulations. Two closed processes P and Q are weakly late HO bisimilar, noted $P \mathrel{\dot{\approx}} Q$, iff there exists a late weak HO bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

As in the strong case, we have:

Theorem 6. *The early and late weak HO bisimilarities are sound.*

The Howe's method is used for both proofs. We only give the proof for the early version in Appendix D.2; the proof is similar for the late version. In this particular case, the input-early and early definitions are the same, and since Howe's method works with input-early bisimulation, it works with this one. The definition is non-delay, however Howe's method still works because of the simplicity of the definition in the concretion case.

We also have completeness of the early version on image-finite processes:

Definition 23. *A process P is image finite iff:*

- *For all first-order label l, the set $\{P_i | P \overset{l}{\Rightarrow} P_i\}$ is finite.*
- *For all higher-order name a, the set $\{F_i | P \overset{a}{\Rightarrow} F_i\}$ is finite and for all F_i in this set and all process R, the set $\{P_i | F_i \circ R \overset{\tau}{\Rightarrow} P_i\}$ is also finite.*
- *For all higher-order name a, the set $\{C_i | P \overset{\overline{a}}{\Rightarrow} C_i\}$ is finite and for all $C_i = \langle R_i \rangle S_i$ in this set, the set $\{S'_i | S_i \overset{\tau}{\Rightarrow} S'_i\}$ is also finite.*

Theorem 7. *The early weak HO bisimilarity is complete on image-finite processes.*

The proof of this theorem can be found in Appendix E. The restriction to image-finite processes is classical in process calculi (e.g. in the π-calculus [15]). Otherwise, the proof technique is the same as in the strong case. In the following, we show that late and early version coincide, hence the late weak context bisimulation is also complete on image-finite processes.

The HO bisimulations definitions are simpler than context bisimulations in HOπP since they do not features any additional contexts and require tests in the abstraction case only. In the following section, we show that this remaining universal quantification is not necessary.

4.3 Normal bisimulation

In this section, we show that testing one process is enough in the abstraction case and we define a sound and complete bisimulation without any universal quantification, similar to Sangiorgi's normal bisimulation.

In HOπ, testing abstractions $(X)P$ and $(X)Q$ with a trigger $\overline{m}.\mathbf{0}$ (where m does not occur in P, Q) is enough as explained in Section 2.5: if $P\{\overline{m}.\mathbf{0}/X\}$ and $Q\{\overline{m}.\mathbf{0}/X\}$ are context bisimilar, then for all R, $P\{R/X\}$ and $Q\{R/X\}$ are context bisimilar. We first show that this result does not hold in HOP. Consider the following processes:

$$P_1 = !a[X] \mid !\overline{a}\langle \mathbf{0} \rangle \mathbf{0} \qquad Q_1 = P_1 \mid X$$

We have $P_1\{\overline{m}.\mathbf{0}/X\} \dot{\sim} Q_1\{\overline{m}.\mathbf{0}/X\}$, but $P_1\{m.n.\mathbf{0}/X\}$ and $Q_1\{m.n.\mathbf{0}/X\}$ (where m, n do not occur in P, Q) are not strong HO bisimilar, i.e. we have found a process R such that $P\{R/X\}$ and $Q\{R/X\}$ are not strong HO bisimilar.

We first give the idea why $P_m = P_1\{\overline{m}.\mathbf{0}/X\}$ and $Q_m = Q_1\{\overline{m}.\mathbf{0}/X\} = \overline{m}.\mathbf{0} \mid P_m$ are HO bisimilar. All transitions from P_m are easily matched by Q_m, and reciprocally for Q_m, except for transition $Q_m \xrightarrow{\overline{m}} \equiv P_m$. It can only be matched by $P_m \xrightarrow{\overline{m}} a[\mathbf{0}] \mid P_m = P'_m$. We now prove that P_m and P'_m are HO bisimilar. We just have to check passivation on a, i.e. transition $P'_m \xrightarrow{\overline{a}} \langle\mathbf{0}\rangle P_m$. It is clearly matched by message sending on a in P_m, i.e. $P_m \xrightarrow{\overline{a}} \langle\mathbf{0}\rangle P_m$. Consequently P_m and Q_m are early strong HO bisimilar.

However $P_{m,n} = P_1\{m.n.\mathbf{0}/X\}$ and $Q_{m,n} = Q_1\{m.n.\mathbf{0}/X\}$ are not strong HO bisimilar. We consider the transition $Q_{m,n} \xrightarrow{m} n.\mathbf{0} \mid P_{m,n} = Q'_{m,n}$, which can only be matched by a transition $P_{m,n} \xrightarrow{m} a[n.\mathbf{0}] \mid P_{m,n} = P'_{m,n}$. Passivation of a in $P'_{m,n}$, i.e. transition $P'_{m,n} \xrightarrow{a} \langle n.\mathbf{0}\rangle P_{m,n}$, can only be matched by $Q'_{m,n} \xrightarrow{a} \langle m.n.\mathbf{0}\rangle Q'_{m,n}$ or $Q'_{m,n} \xrightarrow{a} \langle\mathbf{0}\rangle Q'_{m,n}$. Since $n.\mathbf{0} \not\dot{\sim} m.n.\mathbf{0}$ and $n.\mathbf{0} \not\dot{\sim} \mathbf{0}$, $P'_{m,n}$ and $Q'_{m,n}$ (and consequently $P_{m,n}$ and $Q_{m,n}$) are not strong HO bisimilar.

In the previous example, a process $\overline{m}.\mathbf{0}$ is not enough to distinguish between process variables inside and outside a locality: a $\xrightarrow{\overline{m}}$ transition from a process $\overline{m}.\mathbf{0}$ in a locality can be matched by a $\xrightarrow{\overline{m}}$ transition from a $\overline{m}.\mathbf{0}$ outside any locality. This distinction, however, becomes possible with a process $m.n.\mathbf{0}$. Suppose we have $P\{m.n.\mathbf{0}/X\}$ HO bisimilar to $Q\{m.n.\mathbf{0}/X\}$, with m, n not occurring in P, Q. A $\xrightarrow{m}$ transition in P is matched by a $\xrightarrow{m}$ transition in Q: the two resulting processes P', Q' may now perform one and only one $\xrightarrow{n}$ transition from a process $n.\mathbf{0}$ in an evaluation context. If the process $n.\mathbf{0}$ is in a locality a in P', then it can be send in a message on a after a passivation. The process Q' has to match with a message sending on a; since the contents of the messages are pairwise HO bisimilar, the message from Q' has to contain $n.\mathbf{0}$. Consequently the only occurrence of $n.\mathbf{0}$ was in an evaluation context in Q' and may be sent in a message on a: it is possible if and only if $n.\mathbf{0}$ is in a locality a.

To summarize, when a process $m.n.\mathbf{0}$ in a locality performs a $\xrightarrow{m}$ transition, it has to be matched by a process $m.n.\mathbf{0}$ in a locality with the same name. More precisely, if a process $m.n.\mathbf{0}$ in P performs a $\xrightarrow{m}$ transition and is matched by a process $m.n.\mathbf{0}$ in Q, then the locality hierarchies around $m.n.\mathbf{0}$ in P and Q are the same. This result is a consequence of the following decomposition lemma:

Lemma 5 (Decomposition)**.** *Let P, Q two open processes such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. If $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} = P_n$, then there exists Q' such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\} = Q_n$ and $P_n \dot{\sim}_l Q_n$ (by definition of the bisimulation). Moreover, we are in one of the following cases:*

- *There exists* P_1, Q_1 *such that* $P_n = n.\mathbf{0} \mid P_1$, $Q_n = n.\mathbf{0} \mid Q_1$ *with* $P_1 \dot{\sim}_l Q_1$.
- *There exists* $a_1, \dots a_k$, $P_1 \dots P_{k+1}$, $Q_1 \dots Q_{k+1}$ *such that*

$$P_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$$

and

$$Q_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$$

and for all $1 \leq j \leq k+1$, $P_j \dot{\sim}_l Q_j$.

The lemma gives several results on two matching transitions $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P_n$ and $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q_n$:

- The resulting $n.\mathbf{0}$ is only under parallel compositions and localities (and not under replication or choice operators) in P_n, Q_n.
- If $n.\mathbf{0}$ is not under a locality in P_n, it is not under a locality in Q_n and the processes in parallel with $n.\mathbf{0}$ in P_n, Q_n are bisimilar.
- If $n.\mathbf{0}$ is under a locality hierarchy $a_1, \dots a_k$ in P_n, then it is under the same locality hierarchy in Q_n, and the locality process bodies $P_1, \dots P_{k+1}$, $Q_1, \dots Q_{k+1}$ are pairwise bisimilar.

For instance, if we have $P\{n.\mathbf{0}/X\} = a[b[n.\mathbf{0} \mid P_3] \mid P_2] \mid P_1$, then we have $Q\{n.\mathbf{0}/X\} = a[b[n.\mathbf{0} \mid Q_3] \mid Q_2] \mid Q_1$ with $P_1 \dot{\sim}_l Q_1$, $P_2 \dot{\sim}_l Q_2$, $P_3 \dot{\sim}_l Q_3$. The proof of this result is given in Appendix F.

From this lemma, we can show that testing abstractions with $m.n.\mathbf{0}$ is enough, as stated in the following theorem:

Theorem 8. *Let* P, Q *two open processes such that* $fv(P,Q) \subseteq \{X\}$ *and* m, n *two names which do not occur in* P, Q. *If* $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, *then for all closed processes* R, *we have* $P\{R/X\} \dot{\sim}_l Q\{R/X\}$

Proof. We give here a sketch of the proof. The complete proof can be found in Appendix F. We define

$$\mathcal{R} = \{(P\{R/X\}, Q\{R/X\}), P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}, m, n \text{ not in } P, Q\}$$

and show that $\mathcal{R}$ is a bisimulation. The proof is done by case analysis on the transition performed by $P\{R/X\}$. We briefly give the proof in the case when a copy of R (at position X_i in P) performs a transition $R \xrightarrow{l} R'$ (we have $P\{R/X\} \xrightarrow{l} P'\{R/X\}\{R'/X_i\}$). We want to show that there exists a transition from $Q\{R/X\}$ which stays in the relation $\mathcal{R}$.

In this case, X_i is in an evaluation context, so we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\}$. By bisimilarity hypothesis, there exists a transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$ such that $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \dot{\sim}_l$

$Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$. Consequently X_j is also in an evaluation context, so we have $Q\{R/X\} \xrightarrow{l} Q'\{R/X\}\{R'/X_j\}$.

The Lemma 5 allows us to decompose P' and Q' in localities and parallel compositions, with pairwise bisimilar processes. From this decomposition and using the fact that $\dot{\sim}_l$ is a congruence, we have $P'\{m.n.\mathbf{0}/X\}\{R'/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$, so we have $P'\{R/X\}\{R'/X_i\} \mathcal{R} Q'\{R/X\}\{R'/X_j\}$, hence the result holds.

□

The theorem allows us to define a bisimulation without any universal quantification, similar to the normal bisimulation of Sangiorgi:

Definition 24. *A relation $\mathcal{R}$ on closed processes is a normal simulation iff $P \mathcal{R} Q$ implies:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \mathcal{R} Q'$.*
- *For all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and for two names m, n which do not occur in processes P, Q, we have $F \circ m.n.\mathbf{0} \mathcal{R} F' \circ R$.*
- *For all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S' such that $Q \xrightarrow{\overline{a}} \langle R' \rangle S'$, $R \mathcal{R} R'$ and $S \mathcal{R} S'$.*

A relation $\mathcal{R}$ is a normal bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are normal simulations. Two closed processes P and Q are normal bisimilar, noted $P \dot{\sim}_n Q$, iff there exists a normal bisimulation $\mathcal{R}$ such that $P \mathcal{R} Q$.

As a corollary of Theorem 8, normal bisimilarity coincides with late and early bisimulations.

Corollary 1. $\dot{\sim}_n = \dot{\sim} = \dot{\sim}_l$

Proof. The inclusions $\dot{\sim}_l \subseteq \dot{\sim} \subseteq \dot{\sim}_n$ are easy by definition. The inclusion $\dot{\sim}_n \subseteq \dot{\sim}_l$ is a consequence of Theorem 8.

□

These results may be extended to the weak case:

Theorem 9. *Let P, Q two open processes such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. If $P\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q\{m.n.\mathbf{0}/X\}$, then for all closed processes R, we have $P\{R/X\} \dot{\approx}_l Q\{R/X\}$*

The proof, which can be found in Appendix F.2, is similar to the strong case one, except for some modifications to Lemma 5. We define weak normal bisimilarity as follows:

Definition 25. *A relation $\mathcal{R}$ on closed processes is a weak normal simulation iff $P \mathcal{R} Q$ implies:*

- *For all $P \xrightarrow{l} P'$, there exists Q' such that $Q \xRightarrow{l} Q'$ and $P' \mathcal{R} Q'$.*

- *For all $P \xrightarrow{a} F$, there exists F' such that $Q \stackrel{a}{\Rightarrow} F'$ and for two names m, n which do not occur in processes P, Q, there exists Q' such that $F' \circ m.n.\mathbf{0} \stackrel{\tau}{\Rightarrow} Q'$ and $F \circ m.n.\mathbf{0} \mathrel{\mathcal{R}} Q'$.*
- *For all $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S'', S' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \stackrel{\tau}{\Rightarrow} S'$, $R \mathrel{\mathcal{R}} R'$ and $S \mathrel{\mathcal{R}} S'$.*

A relation $\mathcal{R}$ is a weak normal bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are weak normal simulations. Two closed processes P and Q are weakly normal bisimilar, noted $P \dot{\approx}_n Q$, iff there exists a weak normal bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

As in the strong case, we have

Corollary 2. $\dot{\approx}_n = \dot{\approx} = \dot{\approx}_l$

Hence in HOP, we can define a suitable bisimulation without any universal quantification. We show in the next section that adding back restriction to the calculus foils this approach.

5 Abstractions equivalence in HOπP

In this section, we present counter-examples to show that a simplification similar to the one of Section 4.3 is not possible in HOπP. We prove that testing large sub-classes of processes (*abstraction-free* and *finite* processes) is not enough to guarantee bisimilarity of abstraction.

5.1 Abstraction-free processes

In the following, we omit the trailing null processes to improve readability; m in an agent definition stands for $m.\mathbf{0}$. We also write $\nu ab.P$ for $\nu a.\nu b.P$. Let $\mathbf{0}_m \triangleq \nu x.x.m$. Process $\mathbf{0}_m$ is bisimilar to $\mathbf{0}$ except it has a free name m. We define the following abstractions:

$$
\begin{aligned}
(X)P &\triangleq (X)\nu nb.(b[X \mid \nu m.\overline{a}\langle \mathbf{0}_m \rangle (m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y)) \\
(X)Q &\triangleq (X)\nu mnb.(b[X \mid \overline{a}\langle \mathbf{0} \rangle (m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y))
\end{aligned}
$$

The two abstractions differ in the process emitted on a and in the position of name restriction on m (inside or outside hidden locality b). An abstraction-free process is a process built with the regular HOπP syntax minus message input $a(X)P$.

We remind that $\sim$ is the early strong context bisimilarity (Definition 13).

Lemma 6. *Let R be an abstraction-free process. We have $P\{R/X\} \sim Q\{R/X\}$.*

Since R is abstraction-free, it cannot receive the message emitted by P or Q on a. Passivation of hidden locality b and transitions from R in $P\{R/X\}$ are thus easily matched by the same transitions in $Q\{R/X\}$.

Let $P_{m,R} = \nu nb.(b[R \mid m \mid n \mid \overline{m}.\overline{m}.p] \mid \overline{n}.b(Y)(Y \mid Y))$, F be an abstraction, and $\mathbb{E}$ be an evaluation context such that $m \notin \text{fn}(\mathbb{E}, F)$. We now prove that $P\{R/X\} \xrightarrow{\overline{a}} \nu m.\langle \mathbf{0}_m \rangle P_{m,R}$ is matched by $Q\{R/X\} \xrightarrow{\overline{a}} \langle \mathbf{0} \rangle \nu m.P_{m,R}$, i.e. that we have $\nu m.(F \circ \mathbf{0}_m \mid \mathbb{E}\{P_{m,R}\}) \sim F \circ \mathbf{0} \mid \mathbb{E}\{\nu m.P_{m,R}\}$. Since $m \notin \text{fn}(\mathbb{E}, F)$, there is no interaction between $F, \mathbb{E}$ and $P_{m,R}$, and the inert process $\mathbf{0}_m$ do not interfere either. Hence the possible transitions from $\nu m.(F \circ \mathbf{0}_m \mid \mathbb{E}\{P_{m,R}\})$ are only from $F, \mathbb{E}$, and internal actions in $P_{m,R}$, and are matched by the same transitions in $F \circ \mathbf{0} \mid \mathbb{E}\{\nu m.P_{m,R}\}$.

Abstractions $(X)P$ and $(X)Q$ may have different behaviors with an argument which may receive on a, like $a(Z)q$, where q is a first-order name such that $p \neq q$. By communication on a, we have $Q\{a(Z)q/X\} \xrightarrow{\tau} \nu mnb.(b[q \mid m \mid n \mid \overline{m}.\overline{m}.p] \mid \overline{n}.b(Y)(Y \mid Y)) = Q_1$. Since Q_1 may perform a $\xrightarrow{q}$ transition, it can only be matched by $P\{a(Z)q/X\} \xrightarrow{\tau} \nu nb.(b[\nu m.(q \mid m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y)) = P_1$. Notice that in P_1, the restriction on m remains inside hidden locality b.

After synchronisation on n and passivation on b, we have $Q_1(\xrightarrow{\tau})^2 \nu mnb.(q \mid q \mid m \mid m \mid \overline{m}.\overline{m}.p \mid \overline{m}.\overline{m}.p) = Q_2$ (process inside b in Q_1 is duplicated). After double synchronisation on m, we have $Q_2(\xrightarrow{\tau})^2 \nu mnb.(q \mid q \mid p \mid \overline{m}.\overline{m}.p) = Q_3$, and Q_3 may perform a $\xrightarrow{p}$ transition. These transitions cannot be matched by P_1. Performing the duplication, we have $P_1(\xrightarrow{\tau})^2 \nu nb.(\nu m.(q \mid m \mid \overline{m}.\overline{m}.p) \mid \nu m.(q \mid m \mid \overline{m}.\overline{m}.p)) = P_2$. Each copied sub-process $q \mid m \mid \overline{m}.\overline{m}.p$ of P_2 has its own private copy of m, and we can no longer perform any transition to have the observable p. More generally, the sequence of transitions $Q_1(\xrightarrow{\tau})^4 \xrightarrow{p}$ cannot be matched by P_1, consequently Q_1 and P_1 (and therefore $Q\{a(Z)q/X\}$ and $P\{a(Z)q/X\}$) are not bisimilar.

This counter-example shows that testing abstractions with abstraction-free processes (such as $m.n.\mathbf{0}$) is not enough to potentially distinguish them. Consequently, we have to test abstractions with processes which performs some kind of message input. Notice that this counter-example relies on how scope extrusion is handled; it reminds the one given to explain why restriction and locality operators do not "structurally" commute (Section 3.1). Other scope extrusion semantics (for instance, name restriction is used as fresh name generator, and is always extruded outside localities) make this counter-example fail. In the next sub-section we give other counter-examples which do not rely on scope extrusion.

5.2 Finite Processes

We define finite processes as follows:

Definition 26. *A finite process is a HOπP process built on the following grammar:*

$$P_F ::= \mathbf{0} \;\mid\; P_F \mid P_F \;\mid\; l.P_F \;\mid\; \nu x.P_F \;\mid\; \overline{a}\langle P \rangle P_F \;\mid\; a(X)P_F \;\mid\; a[P_F]$$

Roughly, finite processes cannot initiate an infinite sequence of transitions. Notice that in a message output, the message does not matter and can be a regular process. We do not allow process variable X in the syntax, hence finite process encompass only message inputs $a(X)P_F$ where either $X \notin \mathrm{fv}(P_F)$ or where X appears in emitted messages only (since emitted processes in a message output may be any process). In other words, processes received on input can only be passed around but never activated. With unrestricted message input, we may encode replication (as explained in Section 2) and therefore have infinite sequence of transitions.

We extend the definition to all agents in the following way: a concretion $\nu\widetilde{x}.\langle R\rangle S$ is finite iff S is finite. An abstraction $(X)P$ is finite iff P is finite. We write A_F the set of finite agents. We give some properties of finite agents:

Lemma 7. *Let F be a finite abstraction. For all HOπP processes P, the process $F \circ P$ is finite.*

Let P_F be a finite process:

- *If $P_F \xrightarrow{\alpha} A$ for some α, then A is finite.*
- *The set $\{\alpha | \exists A, P_F \xrightarrow{\alpha} A\}$ is finite.*
- *For all action α, the set $\{A | P_F \xrightarrow{\alpha} A\}$ is finite.*
- *There is no infinite sequence of processes (P_i) such that $P_0 = P_F$ and for all i, $P_i \xrightarrow{l} P_{i+1}$ or $P_i \xrightarrow{\overline{a}} \nu\widetilde{x}.\langle R\rangle P_{i+1}$ or $P_i \xrightarrow{a} F$ with $F \circ P = P_{i+1}$ for some P.*

The first properties are easy by induction on P_F or F. The last one means that there is no infinite sequence of transitions started by P_F. To prove this, we define the *size* of a process, which strictly decreases at each transition step. Details and proofs can be found in Appendix G.

In the following, we use the *depth* of a finite process P_F, defined as the length of the longest sequence of transitions initiated by P_F.

Definition 27. *We define inductively the depth of a finite agent A_F, written $d(A_F)$, as:*

- *$d(P_F) = 0$ if there is no transition from P_F.*
- *$d(P_F) = 1 + \max\{d(A) | \exists \alpha, P_F \xrightarrow{\alpha} A\}$ otherwise.*
- *For all finite concretions $\nu\widetilde{x}.\langle P\rangle P_F$, we have $d(\nu\widetilde{x}.\langle P\rangle P_F) = d(P_F)$.*
- *For all finite abstractions $(X)P_F$, we have $d((X)P_F) = d(P_F)$.*

Properties of Lemma 7 guarantee that $d(A_F)$ exists for all A_F. We may think that the depth of an abstraction depends on the interacting process. It is not the case since process variable may occurs in processes emitted in a message output, and the depth of a concretion takes into account the continuation only. Hence we have the following lemma:

Lemma 8. *Let F be a finite abstraction. For all HOπP processes P, we have $d(F \circ P) = d(F)$*

We now use depth to prove that using finite processes to test bisimilarity of abstractions is not sufficient.

5.3 Counter-examples

In this section, we give counter-examples to show that testing finite processes is not enough to ensure bisimilarity of abstractions. To show this, we define inductively two families of HOπP abstractions $(F_n), (G_n)$, such that for any finite process P_F such that $d(P_F) = n$, the processes $F_n \circ P_F$ and $G_n \circ P_F$ are context bisimilar, but $F_n \circ Q_{n+1}$ and $G_n \circ Q_{n+1}$ (where Q_{n+1} is a process $m_{n+1}. \dots m_1.\mathbf{0}$ with $n+1$ first-order names) are not context bisimilar.

For a a higher-order name and $F = (X)P$ an abstraction, we write $a.F$ for $a(X)P$. Let $\sim$ be HOπP early strong context bisimilarity. We define:

$$F_0 \triangleq (X_0)X_0, G_0 \triangleq (X_0)(X_0 \mid X_0)$$

and for $n > 0$, we define

$$F_n \triangleq (X_n)\nu a_n.(a_n[X_n] \mid a_n.F_{n-1}) + R_n$$

$$G_n \triangleq (X_n)\nu a_n.(a_n[X_n] \mid a_n.G_{n-1}) + S_n$$

with $R_n = \nu a_n.\tau.G_{n-1} \circ X_n$ and $S_n = \nu a_n.\tau.F_{n-1} \circ X_n$. Notice that R_n mimics passivation of locality a_n in G_n, and S_n mimics passivation of a_n in F_n. They have been added to match some particular transitions.

Let (m_k) be a family of pairwise distinct fresh names which do not occur in any F_n nor G_n. Let $Q_1 = m_1.\mathbf{0}$ and $Q_{k+1} = m_{k+1}.Q_k$ for all $k > 1$. Abstractions F_n and G_n are designed such that we have $F_n \circ P_F \sim G_n \circ P_F$ for all P_F such that $d(P_F) \leq n$, but $F_n \circ Q_{n+1}$ is not bisimilar to $G_n \circ Q_{n+1}$. To have an intuition as to why $F_n \circ Q_{n+1}$ and $G_n \circ Q_{n+1}$ are not bisimilar, consider the following sequence of transitions from $F_n \circ Q_{n+1}$: an $\xrightarrow{m_{n+1}}$ transition, followed by a passivation of locality a_n; we obtain $F_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.F_{n-1}) \xrightarrow{\tau}\sim F_{n-1} \circ Q_n$. As this sequence must be matched by $G_n \circ Q_{n+1}$, we obtain $F_{n-1} \circ Q_n$ and $G_{n-1} \circ Q_n$. After repeating this sequence of transitions $n-1$ times, we obtain $F_0 \circ Q_1 = m_1.\mathbf{0}$ and $G_0 \circ Q_1 = m_1.\mathbf{0} \mid m_1.\mathbf{0}$, which are clearly not bisimilar. Consequently $F_n \circ Q_{n+1}$ is not bisimilar to $G_n \circ Q_{n+1}$.

If we do the same with $F_n \circ Q_n$ and $G_n \circ Q_n$, we obtain processes bisimilar to $\mathbf{0}$ and $\mathbf{0} \mid \mathbf{0}$. Another possible evolution is to trigger passivation of a_n directly, without any transition from Q_n beforehand: in this case, we have $F_n \circ Q_n \xrightarrow{\tau} \nu a_n.(F_{n-1} \circ Q_n)$. Process $G_n \circ Q_n$ matches this transition with the τ-action of its sub-process S_n: we have $G_n \circ Q_n \xrightarrow{\tau} \nu a_n.(F_{n-1} \circ Q_n)$. The two resulting processes are identical. All the other evolutions of $F_n \circ Q_n$ are also matched by $G_n \circ Q_n$. More generally, a process P_F which perform less than n transitions cannot distinguish F_n and G_n.

Lemma 9. *If $d(P_F) \leq n$, then $F_n \circ P_F \sim G_n \circ P_F$.*

We prove Lemma 9 by showing that the relation:

$$\mathcal{R}_n \stackrel{\Delta}{=} \{(P\{\widetilde{F_k \circ P_k}/\widetilde{X}\}, P\{\widetilde{G_k \circ P_k}/\widetilde{X}\}), \forall k, d(P_k) \leq k \leq n\}$$

is an early strong context bisimulation. The complete proof may be found in Appendix G. The relation is a bit complex since a process P_F may evolve toward a concretion; consequently we have to introduce a surrounding environment (here P), which may duplicate $F_n \circ P_F$ and $G_n \circ P_F$.

To summarize, testing a finite process P_F with depth n is not enough, since we have $F_n \circ P_F \sim G_n \circ P_F$, but $F_n \circ Q_{n+1} \nsim G_n \circ Q_{n+1}$. Testing a finite set $\mathcal{P}$ of finite processes is not enough either. Since $\mathcal{P}$ is finite, the set $\{d(P_F) | P_F \in \mathcal{P}\}$ is finite and has a greatest element d. For all $P_F \in \mathcal{P}$, we have $F_d \circ P_F \sim G_d \circ P_F$ but $F_d \circ Q_{d+1} \nsim F_d \circ Q_{d+1}$. Similarly, testing an infinite set of finite processes with depths bounded by d is not enough.

Most cases are already covered by the abstraction-free counter-example, except for the abstractions. Besides, the counter-examples of this subsection do not rely on scope extrusion "by need" like the previous one, which means that they may be still valid with other ways to handle scope extrusion. We conjecture that we cannot define a normal bisimilarity in HOπP, i.e. that we cannot define a sound and complete strong bisimilarity with fewer tests than early strong context bisimilarity.

6 Related work

The syntax and semantics of HOP is inspired from the one of HOπ, removing restriction and adding passivation. Sangiorgi studies behavioral equivalences for HOπ in [13]. He defines context and normal bisimilarities as substitutes for barbed bisimilarity. In the message sending and input cases, context bisimilarity considers the possible environments which may communicate with the tested processes. Normal bisimulation improves context bisimulation: in the message sending and input cases, normal bisimilarity tests equivalence with only one process.

The Kell-calculus [16] and Homer [8] are two higher-order calculi with passivation in which bisimulations have been defined. The two calculi share some common concepts, like hierarchical localities, local names, and objective passive and active process mobility. The calculi differ in how they handle communication.

In the Kell-calculus, communications may use join patterns and are only local: processes may communicate only if they are in the same locality or in direct parent-child localities. In the strong case, a sound and complete early context bisimulation has been defined. In the message sending (resp. input) cases (which encompass passivation), this bisimulation considers all the contexts which may receive (resp. send) a message or a kell on the same channel. The complementary action may be performed either at the same level, from a sub-locality, or from a parent locality. Consequently nearly all contexts are tested in the message sending and input cases.

In Homer, a process may send a message to a nested sub-locality or it may passivate it, but the interactions are not allowed in the other way: a process in a sub-locality cannot send a message to a process in a parent one. Passive processes go down in the locality hierarchy (by message sending), and active processes go up (by passivation). In [6], the authors define an *input early* context bisimulation which is sound in the weak case and sound and complete in the strong case. An input-early bisimilarity is late in the message sending case and early in the message input case. As in HOπ or other calculi, context bisimilarity for Homer tests every possible communicating context in the message sending and input cases, but it also features an additional quantification on contexts in the message sending case.

The Seal calculus [18] [5] features a form of process mobility similar to passivation: localities may be stopped, duplicated, and moved up and down in the locality hierarchy. Mobility is less flexible than in Homer or Kell since a process inside a locality cannot be dissociated from its locality boundary. The authors define a bisimilarity in [4] called *Hoe bisimilarity* for the Seal calculus which is similar to normal bisimulation for HOπ in the message sending case. However this Hoe bisimilarity is sound but not complete.

Mobile Ambients [3] is also a higher-order calculus with hierarchical localities. Unlike previous calculi, mobility in Mobile Ambients is subjective: localities move by themselves, without any acknowledgment from their environment. In [10], Merro defines a context bisimilarity which characterizes barbed congruence. A normal bisimulation without universal quantification has yet to be found.

7 Conclusion

Behavioral theory in calculi with passivation (like Homer or the Kell-calculus) is lacking compared to a simpler higher-order calculus like HOπ. Sound and complete context bisimulation have been developed in the strong case only, and they require additional tests on contexts in the message output case. This additional complexity comes from the relationship between name restriction and passivation.

In a calculus with passivation and without name restriction, we have developed and presented normal bisimulations similar to Sangiorgi's for HOπ:

- We introduce a simple higher-order bisimulation which characterizes barbed congruence. In a message output, the message and the continuation are considered separately, since they do not share private names and passivation may put them in different contexts to interact with them independently. Early and late formulations coincide.

- We also introduce a normal bisimulation without any universal quantification which coincides with higher-order bisimulation. HOπ comes from an encoding of higher-process in a first-order, which is not possible in HOP. Instead, our normal bisimulation relies on a means (a process $m.n.\mathbf{0}$) to observe locality hierarchies and to decompose abstractions in bisimilar sub-processes.

However we have not been able to adapt our proof technique to the calculus with restriction. As proved in Section 5, testing any abstraction-free processes is not enough to establish abstractions equivalence. We conjecture that in a calculus featuring passivation and name restriction, we cannot define a sound and complete strong bisimilarity with fewer tests than early strong context bisimilarity.

References

[1] Michael Baldamus. *Semantics and Logic of Higher-Order Processes: Characterizing Late Context Bisimulation*. PhD thesis, Berlin University of Technology, 1998.

[2] Zining Cao. More on bisimulations for higher order pi-calculus. In *FoSSaCS '06*, volume 3921 of *LNCS*, pages 63–78. Springer, 2006.

[3] Luca Cardelli and Andrew D. Gordon. Mobile ambients. In *FoSSaCS '98*, volume 1378 of *LNCS*, pages 140–155. Springer, 1998.

[4] Giuseppe Castagna and Francesco Zappa Nardelli. The seal calculus revisited: Contextual equivalence and bisimilarity. In *FSTTCS '02*, volume 2556 of *LNCS*, pages 85–96. Springer, 2002.

[5] Giuseppe Castagna, Jan Vitek, and Francesco Zappa Nardelli. The Seal Calculus. *Information and Computation*, 201(1):1–54, 2005.

[6] Jens Chr. Godskesen and Thomas Hildebrandt. Extending howe's method to early bisimulations for typed mobile embedded resources with local names. In *FSTTCS '05*, volume 3821 of *LNCS*, pages 140–151. Springer, 2005.

[7] Andrew D. Gordon. Bisimilarity as a theory of functional programming. Mini-course. Notes Series NS-95-3, BRICS, University of Cambridge Computer Laboratory, July 1995. iv+59 pp.

[8] Thomas Hildebrandt, Jens Chr. Godskesen, and Mikkel Bundgaard. Bisimulation congruences for Homer — a calculus of higher order mobile embedded resources. Technical Report ITU-TR-2004-52, IT University of Copenhagen, 2004.

[9] Ivan Lanese, Jorge A. Pérez, Davide Sangiorgi, and Alan Schmitt. On the expressiveness and decidability of higher-order process calculi. In *23rd Annual IEEE Symposium on Logic in Computer Science, LICS 2008*. IEEE Computer Society, 2008.

[10] Massimo Merro and Francesco Zappa Nardelli. Behavioral theory for mobile ambients. *Journal of the ACM*, 52(6):961–1023, 2005.

[11] Robin Milner. *Communicating and Mobile Systems : the π-calculus*. Cambridge University Press, 1999.

[12] Davide Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms*. PhD thesis, Department of Computer Science, University of Edinburgh, 1992.

[13] Davide Sangiorgi. Bisimulation for higher-order process calculi. *Information and Computation*, 131(2):141–178, 1996.

[14] Davide Sangiorgi and Robin Milner. The problem of "weak bisimulation up to". In *3rd International Conference on Concurrency Theory (CONCUR)*, volume 630 of *LNCS*, pages 32–46. Springer, 1992.

[15] Davide Sangiorgi and David Walker. *The Pi-Calculus: A Theory of Mobile Processes*. Cambridge University Press, 2001.

[16] Alan Schmitt and Jean-Bernard Stefani. The Kell Calculus: A Family of Higher-Order Distributed Process Calculi. In *Global Computing 2004 workshop*, volume 3267 of *LNCS*, January 2004.

[17] Bent Thomsen. Plain chocs: A second generation calculus for higher order processes. *Acta Informatica*, 30(1):1–59, 1993.

[18] Jan Vitek and Giuseppe Castagna. Seal: A framework for secure mobile computations. In *ICCL'98: Workshop on Internet Programming Languages*, volume 1686 of *LNCS*, pages 47–77. Springer, 1999.

A Soundness proof for HOπP

In this section, we work with the early bisimulation. Proofs are similar or simpler with the late bisimulation. To prove soundness of early strong bisimilarity with respect to strong barbed congruence, it suffices to show that early strong bisimilarity is a congruence, since early strong bisimilarity is included in strong barbed bisimilarity, and strong barbed congruence is the largest congruence included in strong barbed bisimilarity (by definition).

To prove that a relation is a bisimulation, we use a notion of progress (defined in [15]):

Definition 28. *Let $\mathcal{R}$,$\mathcal{U}$ be binary relations on closed processes. Relation $\mathcal{R}$ is said to* strongly progress towards *$\mathcal{U}$, noted $\mathcal{R} \rightsquigarrow \mathcal{U}$ iff for all closed processes such that $P \mathcal{R} Q$, we have:*

- *If $P \xrightarrow{l} P'$, then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathcal{U} Q'$.*
- *If $P \xrightarrow{a} F$, then for all closed concretions C, there exists F' such that $Q \xrightarrow{a} F'$ and $F \bullet C \, \mathcal{U} \, F' \bullet C$.*
- *If $P \xrightarrow{\overline{a}} C$, for all closed abstractions F, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all evaluation contexts $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \, \mathcal{U} \, F \bullet \mathbb{E}\{C'\}$.*

Lemma 10. *Let $\mathcal{R}$ be a reflexive binary relation on closed processes, let $\mathcal{U}$ be its reflexive and transitive closure. If $\mathcal{R} \rightsquigarrow \mathcal{U}$, then $\mathcal{U}$ is a strong simulation.*

Proof. If $\mathcal{U} \rightsquigarrow \mathcal{U}$, then $\mathcal{U}$ is a simulation. We prove by induction on n that we have $\mathcal{R}^n \rightsquigarrow \mathcal{U}$. There is nothing to show for $n = 1$. We suppose that the result holds for all $k \leq n$. Let $P \, \mathcal{R}^{n+1} \, Q$. Then there exists P_n such that $P \, \mathcal{R}^n \, P_n \, \mathcal{R} \, Q$. We check the conditions of progress:

- If $P \xrightarrow{l} P'$, then by induction there exists P'_n such that $P_n \xrightarrow{l} P'_n$ and $P' \, \mathcal{U} \, P'_n$. Since $\mathcal{R} \rightsquigarrow \mathcal{U}$ and $P_n \, \mathcal{R} \, Q$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P'_n \, \mathcal{U} \, Q'$. Hence we have found Q' such that $Q \xrightarrow{l} Q'$ and $P' \, \mathcal{U}^2 \, Q'$. By transitivity of $\mathcal{U}$, we have $P' \, \mathcal{U} \, Q'$ as required.
- Assume $P \xrightarrow{a} F$ and let C be a closed concretion. By induction, there exists F'_n such that $P_n \xrightarrow{a} F'_n$ and $F \bullet C \, \mathcal{U} \, F'_n \bullet C$. Since $\mathcal{R} \rightsquigarrow \mathcal{U}$ and $P_n \, \mathcal{R} \, Q$, there exists F' such that $Q \xrightarrow{a} F'$ and $F'_n \bullet C \, \mathcal{U} \, F' \bullet C$. We have the result by transitivity of $\mathcal{U}$.
- Assume $P \xrightarrow{\overline{a}} C$, and let F be a closed abstraction. By induction, there exists C'_n such that $P_n \xrightarrow{\overline{a}} C'_n$ and for all evaluation contexts $\mathbb{E}$, $F \bullet \mathbb{E}\{C'_n\} \, \mathcal{U} \, F \bullet \mathbb{E}\{C\}$. Since $\mathcal{R} \rightsquigarrow \mathcal{U}$ and $P_n \, \mathcal{R} \, Q$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}$, $F \bullet \mathbb{E}\{C'_n\} \, \mathcal{U} \, F \bullet \mathbb{E}\{C'\}$. The result holds by transitivity of $\mathcal{U}$.

For all n, we have $\mathcal{R}^n \rightsquigarrow \mathcal{U}$, so we have $\mathcal{U} \rightsquigarrow \mathcal{U}$, and thus $\mathcal{U}$ is a strong context simulation.

□

In the rest of the proof, we define $\mathcal{R}= \{(\mathbb{C}\{P\{\widetilde{Q}/\widetilde{X}\}\}, \mathbb{C}\{P\{\widetilde{R}/\widetilde{X}\}\}), \mathrm{fv}(P) = \widetilde{X}, \widetilde{Q} \sim \widetilde{R}, \mathbb{C}$ closed context$\}$ and its closure $\mathcal{U}=\mathcal{R}^*$. Capture of free names may occur with the restriction operator. This case is not taken into account with the substitution alone (which is capture-free by definition), consequently we add a context $\mathbb{C}$ in the definition of the relation for possible captures.

Lemma 11. *If $P\ \mathcal{U}\ Q$, then for all names x, a, for all closed processes T we have $\nu x.P\ \mathcal{U}\ \nu x.Q, P \mid T\ \mathcal{U}\ Q \mid T, a[P]\ \mathcal{U}\ a[Q]$, $!P\ \mathcal{U}\ !Q$.*

Proof. We proceed by induction on n, proving that $P\ \mathcal{R}^n\ Q$ implies $\nu x.P\ \mathcal{R}^n\ \nu x.Q, P \mid T\ \mathcal{R}^n\ Q \mid T, \ldots$

For $n = 1$, let $P\ \mathcal{R}\ Q$ with $P = \mathbb{C}\{U\{\widetilde{R}/\widetilde{X}\}\}$ and $Q = \mathbb{C}\{U\{\widetilde{S}/\widetilde{X}\}\}$. Since $\nu x.\mathbb{C}, \mathbb{C} \mid T$, $!\mathbb{C}$, and $a[\mathbb{C}]$ are closed contexts, we have $\nu x.P\ \mathcal{R}\ \nu x.Q, P \mid T\ \mathcal{R}\ Q \mid T, !P\ \mathcal{R}\ !Q, a[P]\ \mathcal{R}\ a[Q]$.

Assume now that the result holds up to n. We show that it holds for $n + 1$ in the restriction case (the other cases are similar). Let $P\ \mathcal{R}^{n+1}\ Q$. Then there exists P_n such that $P\ \mathcal{R}^n\ P_n\ \mathcal{R}\ Q$. By induction assumption, we have $\nu x.P\ \mathcal{R}^n\ \nu x.P_n$. Also we have $\nu x.P_n\ \mathcal{R}\ \nu x.Q$, hence we conclude $\nu x.P\ \mathcal{R}^{n+1}\ \nu x.Q$.

□

Lemma 12. *For all closed processes P, P' and for all evolution contexts $\mathbb{G}$, if $P\ \mathcal{U}\ P'$ then $\mathbb{G}\{P\}\ \mathcal{U}\ \mathbb{G}\{P'\}$.*

Proof. By induction on $\mathbb{G}$, using lemma 11. □

For all process P such that $\mathrm{fv}(P) \subseteq \widetilde{X}$ and for all set $\widetilde{R}$ of closed processes with the same number of elements than $\widetilde{X}$, we write $P_{\widetilde{R}}$ for $P\{\widetilde{R}/\widetilde{X}\}$.

Lemma 13. *For all $P_{\widetilde{R}}, P_{\widetilde{S}}$ such that $P_{\widetilde{R}}\ \mathcal{R}\ P_{\widetilde{S}}$, if $P_{\widetilde{R}} \xrightarrow{a} F$, then for all closed processes T such that $fn(T) \cap bn(F) = \emptyset$, there exists F' such that $P_{\widetilde{S}} \xrightarrow{a} F'$ and $F \circ T\ \mathcal{U}\ F' \circ T$.*

Proof. A common subcase is when $P = X$ (the transition comes from R). In this case, we have $R \xrightarrow{a} (F)$ with $R \sim S$. By definition of the bisimulation, there exists F' such that $S \xrightarrow{a} F'$ and $F \bullet \langle T \rangle \mathbf{0} \sim F' \bullet \langle T \rangle \mathbf{0}$, i.e. $F \circ T \sim F' \circ T$. Since $\sim \subseteq \mathcal{U}$, we have the required result.

In the following, we suppose $P \neq X$. We proceed by induction on the derivation $P_{\widetilde{R}} \xrightarrow{a} F$:

- LTS-ABSTR Since $P \neq X$, the derivation comes from P, so $P = a(Y)Q$. Hence we have $P_{\widetilde{R}} = a(Y)Q_{\widetilde{R}} \xrightarrow{a} (Y)Q_{\widetilde{R}}$ and $P_{\widetilde{S}} = a(Y)Q_{\widetilde{S}} \xrightarrow{a} (Y)Q_{\widetilde{S}}$ by LTS-ABSTR. Since $\widetilde{R}$ and $\widetilde{S}$ are closed, we have $Q_{\widetilde{R}}\{T/Y\} = Q\{T/Y\}_{\widetilde{R}}\ \mathcal{R}\ Q\{T/Y\}_{\widetilde{S}} = Q_{\widetilde{S}}\{T/Y\}$, so we have $Q_{\widetilde{R}}\{T/Y\}\ \mathcal{U}\ Q_{\widetilde{S}}\{T/Y\}$ for all T.

- LTS-Par We must have $P_{\widetilde{R}} = U_{\widetilde{R}} \mid V_{\widetilde{R}} \xrightarrow{a} F \mid V_{\widetilde{R}}$ with $U_{\widetilde{R}} \xrightarrow{a} F$. Let T be a closed process. We have $U_{\widetilde{R}} \mathrel{\mathcal{R}} U_{\widetilde{S}}$, so by induction there exists F' such that $U_{\widetilde{S}} \xrightarrow{a} F'$ and $F \circ T \mathrel{\mathcal{U}} F' \circ T$. By LTS-Par we have $P_{\widetilde{S}} \xrightarrow{a} F' \mid V_{\widetilde{S}}$, and by lemma 11 we have $F \circ T \mid V_{\widetilde{R}} \mathrel{\mathcal{U}} F' \circ T \mid V_{\widetilde{R}}$ and $F' \circ T \mid V_{\widetilde{R}} \mathrel{\mathcal{U}} F' \circ T \mid V_{\widetilde{S}}$, so by transitivity we have $(F \mid V_{\widetilde{R}}) \circ T = F \circ T \mid V_{\widetilde{R}} \mathrel{\mathcal{U}} F' \circ T \mid V_{\widetilde{S}} = (F' \mid V_{\widetilde{S}}) \circ T$.

- LTS-Restr We must have $P_{\widetilde{R}} = \nu x.U_{\widetilde{R}} \xrightarrow{a} \nu x.F$ with $a \neq x$ and $U_{\widetilde{R}} \xrightarrow{a} F$. Let T be a closed process such that $x \notin \mathrm{fn}(T)$. We have $U_{\widetilde{R}} \mathrel{\mathcal{R}} U_{\widetilde{S}}$ so by induction there exists F' such that $U_{\widetilde{S}} \xrightarrow{a} F'$ and $F \circ T \mathrel{\mathcal{U}} F' \circ T$. By LTS-Restr we have $P_{\widetilde{S}} \xrightarrow{a} \nu x.F'$, and by lemma 11 we have $\nu x.F \circ T \mathrel{\mathcal{U}} \nu x.F' \circ T$, i.e. $(\nu x.F) \circ T \mathrel{\mathcal{U}} (\nu x.F') \circ T$, since $x \notin \mathrm{fn}(T)$.

- LTS-Loc We must have $P_{\widetilde{R}} = b[U_{\widetilde{R}}] \xrightarrow{a} b[F]$ with $U_{\widetilde{R}} \xrightarrow{a} F$. Let T be a closed process. We have $U_{\widetilde{R}} \mathrel{\mathcal{R}} U_{\widetilde{S}}$ so by induction there exists F' such that $U_{\widetilde{S}} \xrightarrow{a} F'$ and $F \circ T \mathrel{\mathcal{U}} F' \circ T$. By LTS-Loc we have $P_{\widetilde{S}} \xrightarrow{a} b[F']$, and by lemma 11 we have $b[F \circ T] \mathrel{\mathcal{U}} b[F' \circ T]$, i.e. we have $(b[F]) \circ T \mathrel{\mathcal{U}} (b[F']) \circ T$ as required.

- LTS-Replic We must have $P_{\widetilde{R}} = !U_{\widetilde{R}} \xrightarrow{a} F \mid !U_{\widetilde{R}}$ with $U_{\widetilde{R}} \xrightarrow{a} F$. Let T be a closed process. We have $U_{\widetilde{R}} \mathrel{\mathcal{R}} U_{\widetilde{S}}$ so by induction there exists F' such that $U_{\widetilde{S}} \xrightarrow{a} F'$ and $F \circ T \mathrel{\mathcal{U}} F' \circ T$. By LTS-Replic we have $P_{\widetilde{S}} \xrightarrow{a} F' \mid !U_{\widetilde{S}}$, and by lemma 11 we have $F \circ T \mid !U_{\widetilde{R}} \mathrel{\mathcal{U}} F' \circ T \mid !U_{\widetilde{R}} \mathrel{\mathcal{U}} F' \circ T \mid !U_{\widetilde{S}}$, hence by transitivity we have $(F \mid !U_{\widetilde{R}}) \circ T \mathrel{\mathcal{U}} (F' \mid !U_{\widetilde{S}}) \circ T$ as required.

□

Lemma 14 (Substitution lemma)**.** *Let P be a process such that $fv(P) \subset \widetilde{X}$, and let $\widetilde{Q}$ and $\widetilde{R}$ two sets of closed processes with the same number of element than $\widetilde{X}$, and such that $\widetilde{Q} \sim \widetilde{R}$. Then $P\{\widetilde{Q}/\widetilde{X}\} \sim P\{\widetilde{R}/\widetilde{X}\}$.*

Proof. We show that the transitive and reflexive closure $\mathcal{U}$ of $\mathcal{R}$ (defined previously) is a strong simulation. As $\mathcal{U}$ is symmetrical, it will imply that $\mathcal{U}$ is a strong bisimulation. By lemma 10, it suffices to show that $\mathcal{R} \rightsquigarrow \mathcal{U}$.

Let $\mathbb{C}\{P_{\widetilde{Q}}\}, \mathbb{C}\{P_{\widetilde{R}}\} \in \mathcal{R}$. We proceed by induction on $\mathbb{C}$.

★ **Case** $\mathbb{C} = \square$ We proceed by induction on the derivation $P_{\widetilde{Q}} \xrightarrow{\alpha} A_{\widetilde{Q}}$. A common subcase is the case $P = X$, and the derivation comes from Q. In this case, we have $P_{\widetilde{Q}} = Q, P_{\widetilde{R}} = R$ with $Q \sim R$. Since $\sim \subseteq \mathcal{R} \subseteq \mathcal{U}$, we have $Q \mathrel{\mathcal{U}} R$. Therefore we consider $P \neq X$ in the following cases.

LTS-Prefix. In this case, we have $P_{\widetilde{Q}} = l.S_{\widetilde{Q}}$. So $P_{\widetilde{R}} = l.S_{\widetilde{R}}$ and $P_{\widetilde{R}} \xrightarrow{l} S_{\widetilde{R}}$. We have $S_{\widetilde{Q}} \mathrel{\mathcal{R}} S_{\widetilde{R}}$, so we have $S_{\widetilde{Q}} \mathrel{\mathcal{U}} S_{\widetilde{R}}$ as required.

LTS-Abstr. In this case, we have $P_{\widetilde{Q}} = a(Y)S_{\widetilde{Q}}$, and $A_{\widetilde{Q}}$ is an abstraction $F_{\widetilde{Q}} = (Y)S_{\widetilde{Q}}$. Then $P_{\widetilde{R}} = a(Y)S_{\widetilde{R}}$. Let C be a closed concretion. We have

$P_{\widetilde{R}} \xrightarrow{a} F_{\widetilde{R}}$. Since C is closed, we have $F_{\widetilde{Q}} \bullet C = (F \bullet C)_{\widetilde{Q}} \mathcal{R} (F \bullet C)_{\widetilde{R}} = F_{\widetilde{R}} \bullet C$. Hence we have $F_{\widetilde{Q}} \bullet C \,\mathcal{U}\, F_{\widetilde{R}} \bullet C$ as required.

LTS-Concr. In this case, we have $P_{\widetilde{Q}} = \overline{a}\langle S_{\widetilde{Q}}\rangle T_{\widetilde{Q}}$, and $P_{\widetilde{Q}} \longrightarrow \langle S_{\widetilde{Q}}\rangle T_{\widetilde{Q}} = C_{\widetilde{Q}}$. Hence $P_{\widetilde{R}} = \overline{a}\langle S_{\widetilde{R}}\rangle T_{\widetilde{R}}$. Let F be a closed abstraction. We have $P_{\widetilde{R}} \longrightarrow C_{\widetilde{R}}$. Let $\mathbb{E}$ be a closed evaluation context. Since F and $\mathbb{E}$ are closed, we have $F \bullet \mathbb{E}\{C_{\widetilde{Q}}\} = (F \bullet \mathbb{E}\{C\})_{\widetilde{Q}} \;\mathcal{R}\; (F \bullet \mathbb{E}\{C\})_{\widetilde{R}} = F \bullet \mathbb{E}\{C_{\widetilde{R}}\}$. Hence we have $F \bullet \mathbb{E}\{C_{\widetilde{Q}}\} \,\mathcal{U}\, F \bullet \mathbb{E}\{C_{\widetilde{R}}\}$ as required.

LTS-FO. In this case, we have $P_{\widetilde{Q}} = S_{\widetilde{Q}} \mid T_{\widetilde{Q}}$ with $S_{\widetilde{Q}} \xrightarrow{m} U_{\widetilde{Q}}$, $T_{\widetilde{Q}} \xrightarrow{\overline{m}} V_{\widetilde{Q}}$, and $P_{\widetilde{Q}} \xrightarrow{\tau} U_{\widetilde{Q}} \mid V_{\widetilde{Q}}$.

By induction, there exists $U'_{\widetilde{R}}$ such that $S_{\widetilde{R}} \xrightarrow{m} U'_{\widetilde{R}}$ and $U_{\widetilde{Q}} \,\mathcal{U}\, U'_{\widetilde{R}}$, and there exists $V'_{\widetilde{R}}$ such that $T_{\widetilde{R}} \xrightarrow{\overline{m}} V'_{\widetilde{R}}$ and $V_{\widetilde{Q}} \,\mathcal{U}\, V'_{\widetilde{R}}$. By LTS-FO we have $S_{\widetilde{R}} \mid T_{\widetilde{R}} \xrightarrow{\tau} U'_{\widetilde{R}} \mid V'_{\widetilde{R}}$. By lemma 11, we have $U_{\widetilde{Q}} \mid V_{\widetilde{Q}} \,\mathcal{U}\, U'_{\widetilde{R}} \mid V_{\widetilde{Q}} \,\mathcal{U}\, U'_{\widetilde{R}} \mid V'_{\widetilde{R}}$, so by transitivity we have $U_{\widetilde{Q}} \mid V_{\widetilde{Q}} \,\mathcal{U}\, U'_{\widetilde{R}} \mid V'_{\widetilde{R}}$, as required.

LTS-Replic-FO. Similar to the case above.

LTS-HO. In this case, we have $P_{\widetilde{Q}} = S_{\widetilde{Q}} \mid T_{\widetilde{Q}}$ with $S_{\widetilde{Q}} \xrightarrow{a} F_{\widetilde{Q}}$, $T_{\widetilde{Q}} \xrightarrow{\overline{a}} C_{\widetilde{Q}}$. So $P_{\widetilde{Q}} \xrightarrow{\tau} F_{\widetilde{Q}} \bullet C_{\widetilde{Q}}$.

By induction, there exists $F'_{\widetilde{R}}$ such that $S_{\widetilde{R}} \xrightarrow{a} F'_{\widetilde{R}}$ and $F_{\widetilde{Q}} \bullet C_{\widetilde{Q}} \,\mathcal{U}\, F'_{\widetilde{R}} \bullet C_{\widetilde{Q}}$, and there exists $C'_{\widetilde{R}}$ such that $T_{\widetilde{R}} \xrightarrow{\overline{a}} C'_{\widetilde{R}}$ and $F'_{\widetilde{R}} \bullet C_{\widetilde{Q}} \,\mathcal{U}\, F'_{\widetilde{R}} \bullet C'_{\widetilde{R}}$. By LTS-HO we have $S_{\widetilde{R}} \mid T_{\widetilde{R}} \xrightarrow{\tau} F'_{\widetilde{R}} \bullet C'_{\widetilde{R}}$. Moreover we have $F_{\widetilde{Q}} \bullet C_{\widetilde{Q}} \,\mathcal{U}\, F'_{\widetilde{R}} \bullet C_{\widetilde{Q}} \,\mathcal{U}\, F'_{\widetilde{R}} \bullet C'_{\widetilde{R}}$, so by transitivity we have $F_{\widetilde{Q}} \bullet C_{\widetilde{Q}} \,\mathcal{U}\, F'_{\widetilde{R}} \bullet C'_{\widetilde{R}}$, as required.

LTS-Replic-HO. Similar to the case above.

LTS-Passiv. In this case, we have $P_{\widetilde{Q}} = a[S_{\widetilde{Q}}]$ and $A_{\widetilde{Q}} = \langle S_{\widetilde{Q}}\rangle\mathbf{0}$. Let F be a closed abstraction. We have $P_{\widetilde{R}} = a[S_{\widetilde{R}}]$ and $P_{\widetilde{R}} \xrightarrow{\overline{a}} \langle S_{\widetilde{R}}\rangle\mathbf{0}$. For all evaluation context $\mathbb{E}$, we have $F \circ S_{\widetilde{Q}} \mid \mathbb{E}\{\mathbf{0}\} \;\mathcal{R}\; F \circ S_{\widetilde{R}} \mid \mathbb{E}\{\mathbf{0}\}$, hence we have $F \circ S_{\widetilde{Q}} \mid \mathbb{E}\{\mathbf{0}\} \,\mathcal{U}\, F \circ S_{\widetilde{R}} \mid \mathbb{E}\{\mathbf{0}\}$ as required.

LTS-Par. In this case, we have $P_{\widetilde{Q}} = S_{\widetilde{Q}} \mid T_{\widetilde{Q}}$, $A_{\widetilde{Q}} = B_{\widetilde{Q}} \mid T_{\widetilde{Q}}$ with $S_{\widetilde{Q}} \xrightarrow{\alpha} B_{\widetilde{Q}}$. We have to discuss on the shape of $B_{\widetilde{Q}}$:

- $B_{\widetilde{Q}}$ is a process U: then $S_{\widetilde{Q}} \xrightarrow{l} U$. So by induction, there exists U' such that $S_{\widetilde{R}} \xrightarrow{l} U'$ and $U \,\mathcal{U}\, U'$. By rule LTS-Par, we have $P_{\widetilde{R}} \xrightarrow{l} U' \mid T_{\widetilde{R}}$, and by lemma 11, we have $U \mid T_{\widetilde{Q}} \,\mathcal{U}\, U' \mid T_{\widetilde{Q}}$. As $T_{\widetilde{Q}} \,\mathcal{U}\, T_{\widetilde{R}}$, we have $U' \mid T_{\widetilde{Q}} \,\mathcal{U}\, U' \mid T_{\widetilde{R}}$ by lemma 11 again. Finally we have $P_{\widetilde{R}} \xrightarrow{l} U' \mid T_{\widetilde{R}}$ and by transitivity of $\mathcal{U}$, we have $U \mid T_{\widetilde{Q}} \,\mathcal{U}\, U' \mid T_{\widetilde{R}}$ as required.

- $B_{\widetilde{Q}}$ is an abstraction F: then $S_{\widetilde{Q}} \xrightarrow{a} F$. Let $C = \nu\widetilde{y}.\langle V\rangle W$ be a closed concretion. By lemma 13, there exists F' such that $S_{\widetilde{R}} \xrightarrow{a} F'$ and $F \circ V \,\mathcal{U}\, F' \circ V$. By LTS-Par, we have $P_{\widetilde{R}} \xrightarrow{a} F' \mid T_{\widetilde{R}}$. By lemma 11, we have

$(F \mid T_{\widetilde{Q}}) \bullet C = \nu\widetilde{y}.(F \circ V \mid T_{\widetilde{Q}} \mid W) \mathcal{U} \nu\widetilde{y}.(F' \circ V \mid T_{\widetilde{Q}} \mid W)$ and since $T_{\widetilde{Q}} \mathcal{R} T_{\widetilde{R}}$, we have $\nu\widetilde{y}.(F' \circ V \mid T_{\widetilde{Q}} \mid W) \mathcal{U} \nu\widetilde{y}.(F' \circ V \mid T_{\widetilde{R}} \mid W) = (F' \mid T_{\widetilde{R}}) \bullet C$. Hence by transitivity of $\mathcal{U}$, we have $(F \mid T_{\widetilde{Q}}) \bullet C \mathcal{U} (F' \mid T_{\widetilde{R}}) \bullet C$ as required.

- $B_{\widetilde{Q}}$ is a concretion C. Let F be a closed abstraction. By induction, there exists C' such that $S_{\widetilde{R}} \xrightarrow{\overline{a}} C'$ and $F \bullet \mathbb{E}\{C \mid T_{\widetilde{Q}}\} \mathcal{U} F \bullet \mathbb{E}\{C' \mid T_{\widetilde{Q}}\}$ for all evaluation context $\mathbb{E}$ (using progress definition with context $\mathbb{E}\{\square \mid T_{\widetilde{Q}}\}$). Since $T_{\widetilde{Q}} \mathcal{U} T_{\widetilde{R}}$, by lemma 12, we have $F \bullet \mathbb{E}\{C' \mid T_{\widetilde{Q}}\} \mathcal{U} F \bullet \mathbb{E}\{C' \mid T_{\widetilde{R}}\}$. By transitivity, we have $F \bullet \mathbb{E}\{C \mid T_{\widetilde{Q}}\} \mathcal{U} F \bullet \mathbb{E}\{C' \mid T_{\widetilde{R}}\}$, and by LTS-Par we have $P_{\widetilde{R}} \xrightarrow{\overline{a}} C' \mid T_{\widetilde{R}}$ as required.

LTS-Restr. In this case, we have $P_{\widetilde{Q}} = \nu x.S_{\widetilde{Q}}, A_{\widetilde{Q}} = \nu x.B_{\widetilde{Q}}$ with $S_{\widetilde{Q}} \xrightarrow{\alpha} B_{\widetilde{Q}}$. We distinguish three cases:

- $B_{\widetilde{Q}}$ is a process T: hence we have $S_{\widetilde{Q}} \xrightarrow{l} T$. By induction there exists T' such that $S_{\widetilde{R}} \xrightarrow{l} T'$ and $T \mathcal{U} T'$. By rule LTS-Restr we have $P_{\widetilde{R}} \xrightarrow{l} \nu x.T'$ and by lemma 11 we have $\nu x.T \mathcal{U} \nu x.T'$ as required.
- $B_{\widetilde{Q}}$ is an abstraction F: then $S_{\widetilde{Q}} \xrightarrow{a} F$. Let $C = \nu\widetilde{y}.\langle V\rangle W$ be a closed concretion such that $x \notin \mathrm{fn}(V)$. By lemma 13, there exists F' such that $S_{\widetilde{R}} \xrightarrow{a} F'$ and $F \circ V \mathcal{U} F' \circ V$. By LTS-Restr, we have $P_{\widetilde{R}} \xrightarrow{a} \nu x.F'$. By lemma 11, we have $(\nu x.F) \bullet C = \nu\widetilde{y}.(\nu x.(F \circ V) \mid W) \mathcal{U} \nu\widetilde{y}.(\nu x.(F' \circ V) \mid W) = (\nu x.F') \bullet C$ as required.
- $B_{\widetilde{Q}}$ is a concretion C: then $S_{\widetilde{Q}} \xrightarrow{\overline{a}} C$. Let F be a closed abstraction. By induction, there exists C' such that $S_{\widetilde{R}} \xrightarrow{\overline{a}} C'$ and $F \bullet \mathbb{E}\{\nu x.C\} \mathcal{U} F \bullet \mathbb{E}\{\nu x.C'\}$ for all evaluation context $\mathbb{E}$ (using progress definition with $\mathbb{E}\{\nu x.\square\}$). Moreover we have $P_{\widetilde{R}} \xrightarrow{\overline{a}} \nu x.C'$ by LTS-Restr, hence the result holds.

LTS-Loc. In this case, we have $P_{\widetilde{Q}} = a[S_{\widetilde{Q}}]$ with $S_{\widetilde{Q}} \xrightarrow{\alpha} B_{\widetilde{Q}}$. We have three cases to consider:

- $B_{\widetilde{Q}}$ is a process T: we have $S_{\widetilde{Q}} \xrightarrow{l} T$. By induction there exists T' such that $S_{\widetilde{R}} \xrightarrow{l} T'$ and $T \mathcal{U} T'$. By LTS-Loc we have $P_{\widetilde{R}} \xrightarrow{l} a[T']$ and by lemma 11 we have $a[T] \mathcal{U} a[T']$ as required.
- $B_{\widetilde{Q}}$ is an abstraction F: we have $S_{\widetilde{Q}} \xrightarrow{b} F$. Let $C = \nu\widetilde{x}.\langle V\rangle W$ be a closed concretion. By lemma 13, there exists F' such that $S_{\widetilde{R}} \xrightarrow{b} F'$ and $F \circ V \mathcal{U} F' \circ V$. By LTS-Loc, we have $P_{\widetilde{R}} \xrightarrow{b} a[F']$. By lemma 11, we have $(a[F]) \bullet C = \nu\widetilde{y}.(a[F \circ V] \mid W) \mathcal{U} \nu\widetilde{y}.(a[F' \circ V] \mid W) = (a[F']) \bullet C$ as required.

- $B_{\widetilde{Q}}$ is a concretion C: then $S_{\widetilde{Q}} \xrightarrow{\overline{b}} C$. Let F be a closed abstraction. By induction, there exists C' such that $S_{\widetilde{R}} \xrightarrow{\overline{b}} C'$ and $F \bullet \mathbb{E}\{a[C]\} \ \mathcal{U} \ F \bullet \mathbb{E}\{a[C']\}$ for all $\mathbb{E}$ (using progress definition with context $\mathbb{E}\{a[\square]\}$). Moreover we have $P_{\widetilde{R}} \xrightarrow{\overline{b}} a[C']$ by LTS-LOC, hence the result holds.

LTS-REPLIC. In this case, we have $P_{\widetilde{Q}} = !S_{\widetilde{Q}}$ with $S_{\widetilde{Q}} \xrightarrow{\alpha} B_{\widetilde{Q}}$. We have three cases to consider:

- $B_{\widetilde{Q}}$ is a process T: we have $S_{\widetilde{Q}} \xrightarrow{l} T$. By induction there exists T' such that $S_{\widetilde{R}} \xrightarrow{l} T'$ and $T \ \mathcal{U} \ T'$. By LTS-REPLIC we have $P_{\widetilde{R}} \xrightarrow{l} T' \mid !S_{\widetilde{R}}$. By lemma 11 and transitivity of $\mathcal{U}$ we have $T \mid !S_{\widetilde{Q}} \ \mathcal{U} \ T' \mid !S_{\widetilde{R}}$ as required.

- $B_{\widetilde{Q}}$ is an abstraction F: we have $S_{\widetilde{Q}} \xrightarrow{a} F$. Let $C = \nu\widetilde{x}.\langle V\rangle W$ be a closed concretion. By lemma 13, there exists F' such that $S_{\widetilde{R}} \xrightarrow{a} F'$ and $F \circ V \ \mathcal{U} \ F' \circ V$. By LTS-REPLIC, we have $P_{\widetilde{R}} \xrightarrow{a} F' \mid !S_{\widetilde{R}}$. By lemma 11 and transitivity of $\mathcal{U}$, we have $F \mid !S_{\widetilde{Q}} \bullet C = \nu\widetilde{y}.(F \circ V \mid !S_{\widetilde{Q}} \mid W) \ \mathcal{U} \ \nu\widetilde{y}.(F' \circ V \mid !S_{\widetilde{R}} \mid W) = (F' \mid !S_{\widetilde{R}}) \bullet C$ as required.

- $B_{\widetilde{Q}}$ is a concretion C: then $S_{\widetilde{Q}} \xrightarrow{\overline{b}} C$. Let F be a closed abstraction. By induction, there exists C' such that $S_{\widetilde{R}} \xrightarrow{\overline{b}} C'$ and $F \bullet \mathbb{E}\{C \mid !S_{\widetilde{Q}}\} \ \mathcal{U} \ F \bullet \mathbb{E}\{C' \mid !S_{\widetilde{Q}}\}$ for all $\mathbb{E}$ (using progress definition with contexts $\mathbb{E}\{\square \mid !S_{\widetilde{Q}}\}$). Since $S_{\widetilde{Q}} \ \mathcal{U} \ S_{\widetilde{R}}$, by lemma 12, we have $F \bullet \mathbb{E}\{C' \mid !S_{\widetilde{Q}}\} \ \mathcal{U} \ F \bullet \mathbb{E}\{C' \mid !S_{\widetilde{R}}\}$. By transitivity, we have $F \bullet \mathbb{E}\{C \mid !S_{\widetilde{Q}}\} \ \mathcal{U} \ F \bullet \mathbb{E}\{C' \mid !S_{\widetilde{R}}\}$, and by LTS-REPLIC we have $P_{\widetilde{R}} \xrightarrow{\overline{a}} C' \mid !S_{\widetilde{R}}$ as required.

★ **Case** $\mathbb{C} = \mathbb{C}' \mid S$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ may come from the rules LTS-PAR, LTS-HO, LTS-FO or their symmetric. We omit the symmetric cases, since they are similar (for LTS-HO and LTS-FO) or easier (for LTS-PAR).

LTS-PAR. In this case, we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} B_{\widetilde{Q}}$ and $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} B_{\widetilde{Q}} \mid S$. We have to distinguish three cases:

- $B_{\widetilde{Q}}$ is a process T: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{l} T$. By induction there exists T' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{l} T'$ and $T \ \mathcal{U} \ T'$. By LTS-PAR we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{l} T' \mid S$ and by lemma 11, we have $T \mid S \ \mathcal{U} \ T' \mid S$, as required.

- $B_{\widetilde{Q}}$ is an abstraction F: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{a} F$. Let $C = \nu\widetilde{x}.\langle T\rangle V$ be a closed concretion. By lemma 13 there exists F' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{a} F'$ and $F \circ T \ \mathcal{U} \ F' \circ T$. By LTS-PAR we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{a} F' \mid S$ and by lemma 11, we have $\nu\widetilde{x}.(F \circ T \mid S \mid V) \ \mathcal{U} \ \nu\widetilde{x}.(F' \circ T \mid S \mid V)$, i.e. $(F \mid S) \bullet C \ \mathcal{U} \ (F' \mid S) \bullet C$ as required.

- $B_{\widetilde{Q}}$ is a concretion C: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{\overline{a}} C$. Let F be a closed abstraction. By induction there exists C' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} C'$ and for all evaluation context $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C \mid S\} \mathcal{U} F \bullet \mathbb{E}\{C' \mid S\}$. By LTS-PAR we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} C' \mid S$, hence the result holds.

LTS-FO. In this case, we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{l} T$ and $S \xrightarrow{\overline{l}} U$. By induction there exists T' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{l} T'$ and $T \mathcal{U} T'$. By LTS-FO, we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\tau} T' \mid U$, and by lemma 11, we have $T \mid U \mathcal{U} T' \mid U$ as required.

LTS-HO. In this case, we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{a} F$ and $S \xrightarrow{\overline{a}} C$. By induction there exists F' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{a} F'$ and $F \bullet C \mathcal{U} F' \bullet C$. By LTS-HO, we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\tau} F' \bullet C$ as required.

★ **Case** $\mathbb{C} = S \mid \mathbb{C}'$ Similar to the case above.

★ **Case** $\mathbb{C} = \nu x.\mathbb{C}'$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ comes from rule LTS-RESTR:

- $A_{\widetilde{Q}}$ is a process T: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{l} T$ with $l \notin \{x, \overline{x}\}$. By induction there exists T' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{l} T'$ and $T \mathcal{U} T'$. By LTS-RESTR we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{l} \nu x.T'$, and by lemma 11 we have $\nu x.T \mathcal{U} \nu x.T'$ as required.

- $A_{\widetilde{Q}}$ is an abstraction F: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{a} F$ with $a \neq x$. Let $C = \nu\widetilde{y}.\langle T\rangle V$ be a closed concretion such that $x \notin \text{fv}(T)$. By lemma 13 there exists F' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{a} F'$ and $F \circ T \mathcal{U} F' \circ T$. By LTS-RESTR we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{a} \nu x.F'$ and by lemma 11, we have $\nu\widetilde{y}.((\nu x.F) \circ T \mid V) \mathcal{U} \nu\widetilde{y}.((\nu x.F') \circ T \mid V)$, i.e. $(\nu x.F) \bullet C \mathcal{U} (\nu x.F') \bullet C$ as required.

- $A_{\widetilde{Q}}$ is a concretion C: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{\overline{a}} C$ with $a \neq x$. Let F be a closed abstraction. By induction there exists C' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} C'$ and $F \bullet \mathbb{E}\{\nu x.C\} \mathcal{U} F \bullet \mathbb{E}\{\nu x.C'\}$ for all evaluation context $\mathbb{E}$. By LTS-RESTR we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} \nu x.C'$, hence the result holds.

★ **Case** $\mathbb{C} = b[\mathbb{C}']$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ may come from rules LTS-LOC or LTS-PASSIV:

LTS-LOC. In this case we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} B_{\widetilde{Q}}$ and $A_{\widetilde{Q}} = b[B_{\widetilde{Q}}]$. We have three different cases:

- $B_{\widetilde{Q}}$ is a process T: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{l} T$. By induction there exists T' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{l} T'$ and $T \mathcal{U} T'$. By LTS-LOC we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{l} b[T']$ and by lemma 11 we have $b[T] \mathcal{U} b[T']$ as required.

- $B_{\widetilde{Q}}$ is an abstraction F: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{a} F$. Let $C = \nu\widetilde{y}.\langle T\rangle V$ be a closed concretion. By lemma 13 there exists F' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{a} F'$ and $F \circ T \;\mathcal{U}\; F' \circ T$. By LTS-Loc we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{a} b[F']$ and by lemma 11, we have $\nu\widetilde{y}.(b[F] \circ T \mid V) \;\mathcal{U}\; \nu\widetilde{y}.(b[F'] \circ T \mid V)$, i.e. $(b[F]) \bullet C \;\mathcal{U}\; (b[F']) \bullet C$ as required.

- $A_{\widetilde{Q}}$ is a concretion C: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{\overline{a}} C$. Let F be a closed abstraction. By induction there exists C' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} C'$ and $F \bullet \mathbb{E}\{b[C]\} \;\mathcal{U}\; F \bullet \mathbb{E}\{b[C']\}$ for all evaluation context $\mathbb{E}$. By LTS-Loc we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} b[C']$, hence the result holds.

LTS-Passiv. In this case we have $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\overline{b}} \langle \mathbb{C}'\{P_{\widetilde{Q}}\}\rangle\mathbf{0}$. Let F be a closed abstraction. We have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\overline{b}} \langle \mathbb{C}'\{P_{\widetilde{R}}\}\rangle\mathbf{0}$. For all evaluation context $\mathbb{E}$ we have $F \circ \mathbb{C}'\{P_{\widetilde{Q}}\} \mid \mathbb{E}\{\mathbf{0}\} \;\mathcal{U}\; F \circ \mathbb{C}'\{P_{\widetilde{R}}\} \mid \mathbb{E}\{\mathbf{0}\}$, hence the result holds.

★ **Case** $\mathbb{C} = !\mathbb{C}'$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ comes from LTS-Replic, with $A_{\widetilde{Q}} = B_{\widetilde{Q}} \mid !\mathbb{C}'\{P_{\widetilde{Q}}\}$. We have three cases to consider for $B_{\widetilde{Q}}$:

- $B_{\widetilde{Q}}$ is a process T: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{l} T$. By induction there exists T' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{l} T'$ and $T \;\mathcal{U}\; T'$. By LTS-Replic we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{l} T' \mid !\mathbb{C}'\{P_{\widetilde{R}}\}$ and by lemma 11 and transitivity of $\mathcal{U}$, we have $T \mid !\mathbb{C}'\{P_{\widetilde{Q}}\} \;\mathcal{U}\; T' \mid !\mathbb{C}'\{P_{\widetilde{R}}\}$, as required.

- $B_{\widetilde{Q}}$ is an abstraction F: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{a} F$. Let $C = \nu\widetilde{x}.\langle T\rangle V$ be a closed concretion. By lemma 13 there exists F' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{a} F'$ and $F \circ T \;\mathcal{U}\; F' \circ T$. By LTS-Replic we have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{a} F' \mid !\mathbb{C}'\{P_{\widetilde{R}}\}$. By lemma 11 and transitivity of $\mathcal{U}$, we have $\nu\widetilde{x}.(F \circ T \mid !\mathbb{C}'\{P_{\widetilde{Q}}\} \mid V) \;\mathcal{U}\; \nu\widetilde{x}.(F' \circ T \mid !\mathbb{C}'\{P_{\widetilde{R}}\} \mid V)$, i.e. $(F \mid !\mathbb{C}'\{P_{\widetilde{Q}}\}) \bullet C \;\mathcal{U}\; (F' \mid !\mathbb{C}'\{P_{\widetilde{R}}\}) \bullet C$ as required.

- $B_{\widetilde{Q}}$ is a concretion C: we have $\mathbb{C}'\{P_{\widetilde{Q}}\} \xrightarrow{\overline{a}} C$. Let F be a closed abstraction. By induction there exists C' such that $\mathbb{C}'\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} C'$ and for all evaluation context $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C \mid !\mathbb{C}'\{P_{\widetilde{Q}}\}\} \;\mathcal{U}\; F \bullet \mathbb{E}\{C' \mid !\mathbb{C}'\{P_{\widetilde{Q}}\}\}$. Since $!\mathbb{C}'\{P_{\widetilde{Q}}\} \;\mathcal{R}\; !\mathbb{C}'\{P_{\widetilde{R}}\}$, we have $F \bullet \mathbb{E}\{C' \mid !\mathbb{C}'\{P_{\widetilde{Q}}\}\} \;\mathcal{U}\; F \bullet \mathbb{E}\{C' \mid !\mathbb{C}'\{P_{\widetilde{R}}\}\}$, so by transitivity we have $F \bullet \mathbb{E}\{C \mid !\mathbb{C}'\{P_{\widetilde{Q}}\}\} \;\mathcal{U}\; F \bullet \mathbb{E}\{C' \mid !\mathbb{C}'\{P_{\widetilde{R}}\}\}$. By LTS-Replic we also have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} C' \mid !\mathbb{C}'\{P_{\widetilde{R}}\}$, hence the result holds.

★ **Case** $\mathbb{C} = a(Y)\mathbb{C}'$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ comes from rule LTS-Abstr: we have $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{a} (Y)\mathbb{C}'\{P_{\widetilde{Q}}\}$. Let $C = \nu\widetilde{x}.\langle T\rangle U$ be a closed concretion. We have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{a} (X)\mathbb{C}'\{P_{\widetilde{R}}\}$. Since $\widetilde{Q}, \widetilde{R}$ are closed, the variable Y occurs in $\mathbb{C}'$ or P, hence $\mathbb{C}'\{P_{\widetilde{Q}}\}\{T/Y\} = \mathbb{C}''\{P'_{\widetilde{Q}}\}$ and $\mathbb{C}'\{P_{\widetilde{R}}\}\{T/Y\} = \mathbb{C}''\{P'_{\widetilde{R}}\}$ for some $\mathbb{C}''$ and P', so we have $\mathbb{C}'\{P_{\widetilde{Q}}\}\{T/Y\} \mathrel{\mathcal{R}} \mathbb{C}'\{P_{\widetilde{R}}\}\{T/Y\}$. By several applications of lemma 11 we have $\nu\widetilde{x}.(\mathbb{C}'\{P_{\widetilde{Q}}\}\{T/Y\} \mid U) \mathrel{\mathcal{R}} \nu\widetilde{x}.(\mathbb{C}'\{P_{\widetilde{R}}\}\{T/Y\} \mid U)$, i.e. $(Y)\mathbb{C}'\{P_{\widetilde{Q}}\} \bullet C \mathrel{\mathcal{U}} (Y)\mathbb{C}'\{P_{\widetilde{R}}\} \bullet C$ as required.

★ **Case** $\mathbb{C} = \overline{a}\langle\mathbb{C}'\rangle T$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ comes from rule LTS-Concr: we have $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\overline{a}} \langle\mathbb{C}'\{P_{\widetilde{Q}}\}\rangle T$. Let $F = (X)U$ be a closed abstraction. We have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} \langle\mathbb{C}'\{P_{\widetilde{R}}\}\rangle T$, and $F \bullet \langle\mathbb{C}'\{P_{\widetilde{Q}}\}\rangle T = U\{\mathbb{C}'\{P_{\widetilde{Q}}\}/X\} \mid T \mathrel{\mathcal{R}} U\{\mathbb{C}'\{P_{\widetilde{R}}\}/X\} \mid T = F \bullet \langle\mathbb{C}'\{P_{\widetilde{R}}\}\rangle T$, hence the result holds.

★ **Case** $\mathbb{C} = \overline{a}\langle T\rangle\mathbb{C}'$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ comes from rule LTS-Concr: we have $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\overline{a}} \langle T\rangle\mathbb{C}'\{P_{\widetilde{Q}}\}$. Let $F = (X)U$ be a closed abstraction. We have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{\overline{a}} \langle T\rangle\mathbb{C}'\{P_{\widetilde{R}}\}$, and $F \bullet \langle T\rangle\mathbb{C}'\{P_{\widetilde{Q}}\} = U\{T/X\} \mid \mathbb{C}'\{P_{\widetilde{Q}}\} \mathrel{\mathcal{R}} U\{T/X\} \mid \mathbb{C}'\{P_{\widetilde{R}}\} = F \bullet \langle T\rangle\mathbb{C}'\{P_{\widetilde{R}}\}$, hence the result holds.

★ **Case** $\mathbb{C} = l.\mathbb{C}'$ The reduction $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{\alpha} A_{\widetilde{Q}}$ comes from rule LTS-Prefix: we have $\mathbb{C}\{P_{\widetilde{Q}}\} \xrightarrow{l} \mathbb{C}'\{P_{\widetilde{Q}}\}$. We have $\mathbb{C}\{P_{\widetilde{R}}\} \xrightarrow{l} \mathbb{C}'\{P_{\widetilde{R}}\}$ and $\mathbb{C}'\{P_{\widetilde{Q}}\} \mathrel{\mathcal{U}} \mathbb{C}'\{P_{\widetilde{R}}\}$, hence the result holds.

□

We now prove the theorem:

Theorem 10. *If $Q \sim R$ then for all x, a, T, we have $\nu x.Q \sim \nu x.R, Q \mid T \sim R \mid T, a[Q] \sim a[R], a(Y)Q \sim a(Y)R, \overline{a}\langle Q\rangle T \sim \overline{a}\langle R\rangle T, \overline{a}\langle T\rangle Q \sim \overline{a}\langle T\rangle R$, $!Q \sim !R$ and $l.Q \sim l.R$.*

Proof. The result holds by using the substitution lemma with $P = X \mid T, P = a[X], P = a(Y)X, P = \overline{a}\langle X\rangle T, P = \overline{a}\langle T\rangle X, P = !X, P = l.X$. The only case which needs a more detailed proof is the restriction operator one, since using the substitution lemma is not possible when $x \in \mathrm{fn}(Q)$ (no capture occurs in a substitution). In this case, we use the fact that the relation $\mathcal{R}$ defined previously is a bisimulation, with $\mathbb{C} = \nu x.\square$ and $P = X$.

□

B Howe's Method

We give the proofs in the strong case. The proofs for the weak case are similar.

We remind the definition of open extension:

Definition 29. *Let P and Q be two open processes. We have $P \mathrel{\mathcal{R}^\circ} Q$ iff $P\sigma \mathrel{\mathcal{R}} Q\sigma$ for all substitutions that close P and Q.*

$$X \mathrel{\widehat{\mathcal{R}}} X \qquad \mathbf{0} \mathrel{\widehat{\mathcal{R}}} \mathbf{0} \qquad \frac{P \mathrel{\mathcal{R}} Q}{l.P \mathrel{\widehat{\mathcal{R}}} l.Q} \qquad \frac{P \mathrel{\mathcal{R}} Q}{\nu x.P \mathrel{\widehat{\mathcal{R}}} \nu x.Q} \qquad \frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{P_1 \mid P_2 \mathrel{\widehat{\mathcal{R}}} Q_1 \mid Q_2}$$

$$\frac{P \mathrel{\mathcal{R}} Q}{a(X)P \mathrel{\widehat{\mathcal{R}}} a(X)Q} \qquad \frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{\overline{a}\langle P_1\rangle P_2 \mathrel{\widehat{\mathcal{R}}} \overline{a}\langle Q_1\rangle Q_2} \qquad \frac{P \mathrel{\mathcal{R}} Q}{a[P] \mathrel{\widehat{\mathcal{R}}} a[Q]} \qquad \frac{P \mathrel{\mathcal{R}} Q}{!P \mathrel{\widehat{\mathcal{R}}} !Q}$$

$$\frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{\langle P_1\rangle P_2 \mathrel{\widehat{\mathcal{R}}} \langle Q_1\rangle Q_2} \qquad \frac{C_1 \mathrel{\mathcal{R}} C_2}{\nu x.C_1 \mathrel{\widehat{\mathcal{R}}} \nu x.C_2}$$

Figure 7: Compatible refinement for processes and concretions

We extends open extension to concretions: we have $C \mathrel{\mathcal{R}^\circ} C'$ iff for all F, we have $F \bullet C \mathrel{\mathcal{R}^\circ} F \bullet C'$

We remind the definition of the Howe closure:

Definition 30. *The Howe's closure is inductively defined by the following rule:*

$$\frac{P \mathrel{\widehat{\mathcal{R}^\bullet}} Q \qquad Q \mathrel{\mathcal{R}^\circ} R}{P \mathrel{\mathcal{R}^\bullet} R}\ \textsc{Def}$$

The compatible refinement for our calculus and its extension to concretions is given Figure 7. We first prove some general properties about the Howe closure:

Lemma 15. *If $\mathcal{R}$ is an equivalence, then $\mathcal{R}^\bullet$ is reflexive and:*

$$\frac{P \mathrel{\widehat{\mathcal{R}^\bullet}} Q}{P \mathrel{\mathcal{R}^\bullet} Q}\ \textsc{Cong} \qquad \frac{P \mathrel{\mathcal{R}^\circ} Q}{P \mathrel{\mathcal{R}^\bullet} Q}\ \textsc{Open} \qquad \frac{P \mathrel{\mathcal{R}^\bullet} Q \qquad Q \mathrel{\mathcal{R}^\circ} R}{P \mathrel{\mathcal{R}^\bullet} R}\ \textsc{Open right}$$

$$\frac{P \mathrel{\mathcal{R}^\bullet} Q \qquad P' \mathrel{\mathcal{R}^\bullet} Q'}{P\{P'/X\} \mathrel{\mathcal{R}^\bullet} Q\{Q'/X\}}\ \textsc{Subst}$$

And the transitive and reflexive closure of $\mathcal{R}^\bullet$ is symmetric Symm.

Proof. The reflexivity can be shown by a direct structural induction on P, using the reflexivity of $\mathcal{R}^\circ$ (since $\mathcal{R}$ is an equivalence). The rule Cong follows from the definition of the Howe closure since $\mathcal{R}^\circ$ is reflexive. By structural induction on P, we can prove that $P \mathrel{\widehat{\mathcal{R}}} P$, hence Open follows from the definition of the Howe closure.

For Open right, assume we have P, Q, R such that $P \mathrel{\mathcal{R}^\bullet} Q$ and $Q \mathrel{\mathcal{R}^\circ} R$. By definition there exists Q' such that $P \mathrel{\widehat{\mathcal{R}^\bullet}} Q'$ and $Q' \mathrel{\mathcal{R}^\circ} Q$. By transitivity of $\mathcal{R}^\circ$, we have $Q\ \mathcal{R}^\circ\ R$, hence we have $P\ \mathcal{R}^\bullet\ R$ as required.

We now prove the rule Subst. Let P, Q, P', Q' such that $P\ \mathcal{R}^\bullet\ Q$ and $P'\ \mathcal{R}^\bullet\ Q'$. We proceed by induction on P:

- $P = \mathbf{0}$: by definition of the Howe closure and the compatible refinement relation, we have $\mathbf{0}\ \mathcal{R}^\circ\ Q$. By definition of the open extension, we have $\mathbf{0}\ \mathcal{R}^\circ\ Q\{Q'/X\}$, so by Open we have $\mathbf{0}\ \mathcal{R}^\bullet\ Q\{Q'/X\}$ as required.
- $P = X$: by definition of the Howe closure and the compatible refinement relation, we have $X\ \mathcal{R}^\circ\ Q$. For all substitution σ that closes Q' we have $X\{Q'\sigma/X\} = Q'\sigma\ \mathcal{R}\ Q\{Q'\sigma/X\}$, so we have $Q'\ \mathcal{R}^\circ\ Q\{Q'/X\}$. We have $P'\ \mathcal{R}^\bullet\ Q'$, so by Open right we have $P'\ \mathcal{R}^\bullet\ Q\{Q'/X\}$ as required.
- $P = \nu x.R$. Since substitution is capture free, we have $x \notin \mathrm{fn}(P')$ and $x \notin \mathrm{fn}(P')$ (by α-conversion if needed). By definition of the Howe closure, there exists R' such that $R\ \mathcal{R}^\bullet\ R'$ and $\nu x.R'\ \mathcal{R}^\circ\ Q$. By induction we have $R\{P'/X\}\ \mathcal{R}^\bullet\ R'\{Q'/X\}$, hence we have $\nu x.R\{P'/X\}\ \widehat{\mathcal{R}^\bullet}\ \nu x.R'\{Q'/X\}$. As $x \notin \mathrm{fn}(P')$ and $x \notin \mathrm{fn}(Q')$, it is the same as $(\nu x.R)\{P'/X\}\ \widehat{\mathcal{R}^\bullet}\ (\nu x.R')\{Q'/X\}$. Since $\nu x.R'\ \mathcal{R}^\circ\ Q$, for all substitutions σ_1 such that $Q'\sigma_1$ is closed and for all substitutions σ_2 such that $R'\{Q'\sigma_1/X\}\sigma_2$ and $Q\{Q'\sigma_1/X\}\sigma_2$ are closed, we have $\nu x.R'\{Q'\sigma_1/X\}\sigma_2\ \mathcal{R}\ Q\{Q'\sigma_1/X\}\sigma_2$, i.e. $\nu x.R'\{Q'/X\}\ \mathcal{R}^\circ\ Q\{Q'/X\}$. Hence by definition of the Howe closure we have $P\{P'/X\}\ \mathcal{R}^\bullet\ Q\{Q'/X\}$.

The other induction cases are similar to the $\nu x.R$ case.

For Symm, we prove that $(\mathcal{R}^\bullet)^{-1} \subseteq (\mathcal{R}^\bullet)^*$. For all B, we show by induction on B that for all A, $A(\mathcal{R}^\bullet)^{-1}B$ implies $A(\mathcal{R}^\bullet)^*B$. We give the proof in one case, the others are similar. Assume $B = \nu a.B'$. We have $\nu a.B'\ \mathcal{R}^\bullet\ A$, so by definition there exists R such that $B'\ \mathcal{R}^\bullet\ R$ and $\nu a.R\ \mathcal{R}^\circ\ A$. Hence we have $R(\mathcal{R}^\bullet)^{-1}B'$, so by induction we have $R(\mathcal{R}^\bullet)^*B'$. By Cong we have $\nu a.R(\mathcal{R}^\bullet)^*\nu a.B'$. Since $\mathcal{R}$ is an equivalence, $\mathcal{R}^\circ$ is symmetric, so we have $A\ \mathcal{R}^\circ\ \nu a.R$, so by Open we have $A\ \mathcal{R}^\bullet\ \nu a.R$. Finally we have $A\ \mathcal{R}^\bullet\ \nu a.R(\mathcal{R}^\bullet)^*\nu a.B'$, i.e. $A(\mathcal{R}^\bullet)^*B$ as required.

□

We now prove a modified simulation property for the restriction of the Howe closure to closed process. We have to extend the Howe closure to evaluation contexts $\mathbb{E}$, which can be easily done by adding the rule

$$\square\ \widehat{\mathcal{R}}\ \square$$

to the compatible refinement relation definition. If $\mathbb{E} \sim_{ie}^\bullet \mathbb{E}'$, then for all a, x, P, Q such that $P \sim_{ie}^\bullet Q$, we have $\mathbb{E}\{\square \mid P\} \sim_{ie}^\bullet \mathbb{E}'\{\square \mid Q\}, \mathbb{E}\{\nu x.\square\} \sim_{ie}^\bullet \mathbb{E}'\{\nu x.\square\}$ and $\mathbb{E}\{a[\square]\} \sim_{ie}^\bullet \mathbb{E}'\{a[\square]\}$. To prove this, we can show by induction that if X do not occur in $\mathbb{E}, \mathbb{E}'$, then $\mathbb{E}\{X\} \sim_{ie}^{\bullet} \mathbb{E}'\{X\}$, and we use rule Subst to conclude.

Let $P\ (\sim_{ie})_c^{\bullet}\ Q$. When we introduce an intermediate process P' using Howe's closure definition, (i.e. such that $P \hat{\sim}_{ie}^{\bullet} P'$ and $P' \sim_{ie}^{\circ} Q$), P' may be open. We show that we can always chosed a closed one.

Lemma 16. *Let $P\ (\sim_{ie})_c^{\bullet}\ Q$. There exists closed process R such that $P \hat{\sim}_{ie}^{\bullet} R$ and $R \sim_{ie}^{\circ} Q$.*

Let $C\ (\sim_{ie})_c^{\bullet}\ D$. There exists closed concretion C' such that $C \hat{\sim}_{ie}^{\bullet} C'$ and $C' \sim_{ie}^{\circ} D$.

Proof. We proceed by induction on P.

- $P = l.P'$. By definition there exists R such that $P' \sim_{ie}^{\bullet} R$ and $l.R \sim_{ie}^{\circ} Q$. The process R may be open; let σ be a substitution which closes R. By reflexivity and Subst, we have $P' \sim_{ie}^{\bullet} R\sigma$ (since P' is closed), and since Q is closed we have $l.R\sigma \sim_{ie} Q$. Since the involved processes are closed, we have $l.R\sigma \sim_{ie}^{\circ} Q$. The process $(l.R)\sigma$ is closed and respect the definition.

- $P = (X)P'$. By definition there exists R such that $P' \sim_{ie}^{\bullet} R$ and $(X)R \sim_{ie}^{\circ} Q$. The process R may be open; let σ be a substitution which closes R, except for variable X. By reflexivity and Subst, we have $P' \sim_{ie}^{\bullet} R\sigma$ (since $\mathrm{fv}(P') \subseteq \{X\}$), and since Q is closed we have $((X)R)\sigma \sim_{ie} Q$. Since the involved processes are closed, we have $((X)R)\sigma \sim_{ie}^{\circ} Q$. The process $((X)R)\sigma$ is closed and respect the definition.

The other cases as well as the concretion case, are similar to the $l.P'$ one.

□

Consequently, in the proofs of the following results, we implicitely use Lemma 16 and introduce closed processes only. Besides we use $(\sim_{ie})_c^{\bullet}$ instead of $\sim_{ie}^{\bullet}$ and $\sim_{ie}^{\circ}$ instead of using $\sim_{ie}$ directly when possible to shorten the proofs.

Lemma 17. *Let $C\ (\sim_{ie})_c^{\bullet}\ C'$ and $P \sim_{ie}^{\bullet} P'$ with $fv(P) = fv(P') \subseteq \{X\}$. We have $(X)P \bullet C\ (\sim_{ie})_c^{\bullet}\ (X)P' \bullet C'$.*

Proof. By induction on $C\ (\sim_{ie})_c^{\bullet}\ C'$. We have two possibilities:

- We have $C = \langle R \rangle S$, $R\ (\sim_{ie})_c^{\bullet}\ R'$, $S\ (\sim_{ie})_c^{\bullet}\ S'$ and $\langle R' \rangle S' \sim_{ie}^{\circ} C'$. Since $P \sim_{ie}^{\bullet} P'$, we have $P\{R/X\}\ (\sim_{ie})_c^{\bullet}\ P'\{R'/X\}$ by Subst. Using Cong we have $P\{R/X\} \mid S\ (\sim_{ie})_c^{\bullet}\ P'\{R'/X\} \mid S'$, i.e. $(X)P \bullet C\ (\sim_{ie})_c^{\bullet}\ (X)P' \bullet \langle R' \rangle S'$. By definition, we have $F \bullet \langle R' \rangle S' \sim_{ie}^{\circ} F \bullet C'$ for all F, in particular we have $(X)P' \bullet \langle R' \rangle S' \sim_{ie}^{\circ} (X)P' \bullet C'$. We then have the required result by Open right.

- We have $C = \nu x.D$, $D\ (\sim_{ie})_c^{\bullet}\ D'$, $\nu x.D' \sim_{ie}^{\circ} C'$. By induction, we have $(X)P \bullet D\ (\sim_{ie})_c^{\bullet}\ (X)P' \bullet D'$. Using Cong (and making several cases depending x is free in the processes emitted by D, D' or not), we have

$(X)P \bullet \nu x.D \;(\sim_{ie})^\bullet_c\; (X)P' \bullet \nu x.D'$. By definition, we have $F \bullet \nu x.D' \sim^\circ_{ie} F \bullet C'$ for all F, in particular we have $(X)P' \bullet \nu x.D' \sim^\circ_{ie} (X)P' \bullet C'$. We then have the required result by Open right

□

Lemma 18. *Let $(\sim_{ie})^\bullet_c$ be the restriction of $\sim^\bullet_{ie}$ to closed terms. If $P \;(\sim_{ie})^\bullet_c\; Q$ then:*

- *If $P \xrightarrow{l} P'$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \;(\sim_{ie})^\bullet_c\; Q'$.*
- *If $P \xrightarrow{a} F$, for all closed concretions $C \;(\sim_{ie})^\bullet_c\; C'$ and evaluation contexts $\mathbb{E} \sim^\bullet_{ie} \mathbb{E}'$, there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}\{F\} \bullet C \;(\sim_{ie})^\bullet_c\; \mathbb{E}'\{F'\} \bullet C'$*
- *If $P \xrightarrow{\overline{a}} C$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all closed evaluation contexts $\mathbb{E}, \mathbb{E}'$ such that $\mathbb{E} \sim^\bullet_{ie} \mathbb{E}'$, we have $\mathbb{E}\{C\} \;(\sim_{ie})^\bullet_c\; \mathbb{E}'\{C'\}$.*

Proof. Let P, Q be processes such that $P \;(\sim_{ie})^\bullet_c\; Q$ and $P \xrightarrow{\alpha} A$. We proceed by induction on the derivation $P \xrightarrow{\alpha} A$.

LTS-Prefix. $P = l.P' \xrightarrow{l} P'$. By definition there exists R such that $P' \sim^\bullet_{ie} R$ and $l.R \sim^\circ_{ie} Q$. By LTS-Prefix we have $l.R \xrightarrow{l} R$, so there exists Q' such that $Q \xrightarrow{l} Q'$ and $R \sim^\circ_{ie} Q'$. By Open right we have $P' \sim^\bullet_{ie} Q'$, and since P' and Q' are closed, we have $P' \;(\sim_{ie})^\bullet_c\; Q'$ as required.

LTS-Abstr. $P = a(X)P' \xrightarrow{a} (X)P'$. By definition there exists R such that $P' \sim^\bullet_{ie} R$ and $a(X)R \sim^\circ_{ie} Q$. Let $C \;(\sim_{ie})^\bullet_c\; C'$ and $\mathbb{E} \;(\sim_{ie})^\bullet_c\; \mathbb{E}'$ be closed evaluation context. By LTS-Abstr we have $a(X)R \xrightarrow{a} (X)R$, so by bisimilarity there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}'\{(X)R\} \bullet C' \sim^\circ_{ie} \mathbb{E}'\{F'\} \bullet C'$.

By Subst, we have $\mathbb{E}\{P'\} \;(\sim_{ie})^\bullet_c\; \mathbb{E}'\{R\}$. By lemma 17, we have $\mathbb{E}\{(X)P'\} \bullet C \;(\sim_{ie})^\bullet_c\; \mathbb{E}'\{(X)R\} \bullet C'$. We have the required result by Open right.

LTS-Concr. $P = \overline{a}\langle R\rangle S \xrightarrow{\overline{a}} \langle R\rangle S$. By definition there exists R', S' such that $R \sim^\bullet_{ie} R', S \sim^\bullet_{ie} S'$ and $\overline{a}\langle R'\rangle S' \sim^\circ_{ie} Q$. By LTS-Concr we have $\overline{a}\langle R'\rangle S' \xrightarrow{\overline{a}} \langle R'\rangle S'$, so there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $F, \mathbb{E}$, we have $F \bullet \mathbb{E}\{\langle R'\rangle S'\} \sim_{ie} F \bullet \mathbb{E}\{C'\}$.

Let $\mathbb{E}, \mathbb{E}'$ be evaluation contexts such that $\mathbb{E} \;(\sim_{ie})^\bullet_c\; \mathbb{E}'$. We have $\mathbb{E}\{S\} \;(\sim_{ie})^\bullet_c\; \mathbb{E}'\{S'\}$. We also have $R \;(\sim_{ie})^\bullet_c\; R'$ so by Cong, we have $\langle R\rangle\mathbb{E}\{S\} \;(\sim_{ie})^\bullet_c\; \langle R'\rangle\mathbb{E}'\{S'\}$. We have the required result by Open right.

LTS-Par. $P = R \mid S \xrightarrow{\alpha} A \mid S$ with $R \xrightarrow{\alpha} A$. By definition there exists R', S' such that $R \sim^\bullet_{ie} R', S \sim^\bullet_{ie} S'$ and $R' \mid S' \sim^\circ_{ie} Q$. We have three cases to consider for A:

- A is a process T: therefore we have $R \xrightarrow{l} T$. By induction, there exists T' such that $R' \xrightarrow{l} T'$ and $T \;(\sim_{ie})^\bullet_c\; T'$. By rule LTS-Par we have $R' \mid S' \xrightarrow{l} T' \mid S'$, and since $R' \mid S' \sim_{ie} Q$, there exists Q' such that

$Q \xrightarrow{l} Q'$ and $T' \mid S' \sim^{\circ}_{ie} Q'$. Using Cong, we have $T \mid S \sim^{\bullet}_{ie} T' \mid S'$, so by Open right we have $T \mid S \; (\sim_{ie})^{\bullet}_{c} \; Q'$ as required.

- A is an abstraction F: therefore we have $R \xrightarrow{a} F$. Let $C \; (\sim_{ie})^{\bullet}_{c} \; C'$ be closed concretions and $\mathbb{E} \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'$ be closed evaluation contexts. Since $\mathbb{E}\{\square \mid S\} \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'\{\square \mid S'\}$, by induction, there exists G such that $R' \xrightarrow{a} G$ and $\mathbb{E}\{F \mid S\} \bullet C \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'\{G \mid S'\} \bullet C'$. By rule LTS-Par we have $R' \mid S' \xrightarrow{a} G \mid S'$, and since $R' \mid S' \sim^{\circ}_{ie} Q$, there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}'\{G \mid S'\} \bullet C \sim^{\circ}_{ie} \mathbb{E}'\{F'\} \bullet C'$. We have the required result by Open right.

- A is a concretion C: therefore we have $R \xrightarrow{\overline{a}} C$. By induction, there exists D such that $R' \xrightarrow{\overline{a}} D$ and for all $\mathbb{E}$, $\mathbb{E}'$ with $\mathbb{E} \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'$, we have $\mathbb{E}\{C\} \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'\{D\}$. By rule LTS-Par we have $R' \mid S' \xrightarrow{\overline{a}} D \mid S'$, and since we have $R' \mid S' \sim^{\circ}_{ie} Q$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}'$, we have $\mathbb{E}'\{D \mid S'\} \sim^{\circ}_{ie} \mathbb{E}'\{C'\}$.

  Let $\mathbb{E}$, $\mathbb{E}'$ be closed evaluation contexts such that $\mathbb{E} \sim^{\bullet}_{ie} \mathbb{E}'$. Since $S \sim^{\bullet}_{ie} S'$, we have $\mathbb{E}\{\square \mid S\} \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'\{\square \mid S'\}$, hence we have $\mathbb{E}\{C \mid S\} \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'\{D \mid S'\}$ by induction hypothesis. The result then holds with rule Open right.

LTS-FO. $P = R \mid S \xrightarrow{\tau} U \mid V$ with $R \xrightarrow{m} U$ and $S \xrightarrow{\overline{m}} V$ for some m. By definition there exists R', S' such that $R \sim^{\bullet}_{ie} R', S \sim^{\bullet}_{ie} S'$ and $R' \mid S' \sim^{\circ}_{ie} Q$. By induction, there exists U', V' such that $R' \xrightarrow{m} U'$ and $S' \xrightarrow{\overline{m}} V'$ such that $U \; (\sim_{ie})^{\bullet}_{c} \; U'$ and $V \; (\sim_{ie})^{\bullet}_{c} \; V'$. By LTS-FO we have $R' \mid S' \xrightarrow{\tau} U' \mid V'$. Since $R' \mid S' \sim^{\circ}_{ie} Q$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $U' \mid V' \sim^{\circ}_{ie} Q'$.

We have $U \; (\sim_{ie})^{\bullet}_{c} \; U'$ and $V \; (\sim_{ie})^{\bullet}_{c} \; V'$, so by Cong, we have $U \mid V \sim^{\bullet}_{ie} U' \mid V'$. By Open right we have $U \mid V \; (\sim_{ie})^{\bullet}_{c} \; Q'$ as required.

LTS-Replic-FO. Similar to the case above.

LTS-HO. $P = R \mid S \xrightarrow{\tau} F \bullet C$, with $R \xrightarrow{a} F$ and $S \xrightarrow{\overline{a}} C$ for some a. By definition there exists R', S' such that $R \sim^{\bullet}_{ie} R', S \sim^{\bullet}_{ie} S'$ and $R' \mid S' \sim^{\circ}_{ie} Q$.

By induction, there exists C' such that $S' \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}$, $\mathbb{E}'$, such that $\mathbb{E} \; (\sim_{ie})^{\bullet}_{c} \; \mathbb{E}'$, we have $\mathbb{E}\{C\} \sim^{\bullet}_{ie} \mathbb{E}'\{C'\}$. In particular we have $C \sim^{\bullet}_{ie} C'$. Since we have $R \; (\sim_{ie})^{\bullet}_{c} \; R'$, there exists F' such that $R' \xrightarrow{a} F'$ and $F \bullet C \; (\sim_{ie})^{\bullet}_{c} \; F' \bullet C'$ (with $\square$ as evaluation contexts).

By rule LTS-HO we have $R' \mid S' \xrightarrow{\tau} F' \bullet C'$. From $R' \mid S' \sim^{\circ}_{ie} Q$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $F' \bullet C' \sim^{\circ}_{ie} Q'$. Finally, we have the required result by Open right.

LTS-Replic-HO. Similar to the case above.

LTS-Restr. $P = \nu x.R \xrightarrow{\alpha} \nu x.A$, with $R \xrightarrow{\alpha} A$ and $\alpha \notin \{x, \overline{x}\}$. By definition there exists R' such that $R \sim^{\bullet}_{ie} R'$ and $\nu x.R' \sim^{\circ}_{ie} Q$. We now distinguish three cases for A:

- A is a process T: therefore we have $R \xrightarrow{l} T$. By induction, there exists T' such that $R' \xrightarrow{l} T'$ and $T\ (\sim_{ie})^\bullet_c\ T'$. By rule LTS-RESTR we have $\nu x.R' \xrightarrow{l} \nu x.T'$, and since $\nu x.R' \sim^\circ_{ie} Q$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $\nu x.T' \sim^\circ_{ie} Q'$. Using CONG, we have $\nu x.T \sim^\bullet_{ie} \nu x.T'$, so by OPEN RIGHT we have $\nu x.T\ (\sim_{ie})^\bullet_c\ Q'$ as required.

- A is an abstraction F: therefore we have $R \xrightarrow{a} F$. Let $C\ (\sim_{ie})^\bullet_c\ C'$ be closed concretions and $\mathbb{E}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'$ be closed evaluation contexts. By induction, there exists G such that $R' \xrightarrow{a} G$ and $\mathbb{E}\{\nu x.F\} \bullet C\ (\sim_{ie})^\bullet_c\ \mathbb{E}'\{\nu x.G\} \bullet C'$. By rule LTS-RESTR we have $\nu x.R' \xrightarrow{a} \nu x.G$, and since $\nu x.R' \sim^\circ_{ie} Q$, there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}'\{\nu x.G\} \bullet C' \sim^\circ_{ie} \mathbb{E}'\{F'\} \bullet C'$. We have the required result by OPEN RIGHT.

- A is a concretion C: therefore we have $R \xrightarrow{\overline{a}} C$. By induction, there exists D such that $R' \xrightarrow{\overline{a}} D$ and for all $\mathbb{E}$, $\mathbb{E}'$ with $\mathbb{E}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'$, we have $\mathbb{E}\{C\}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'\{D\}$. For $\mathbb{E} \sim^\bullet_{ie} \mathbb{E}'$, we have $\mathbb{E}\{\nu x.\Box\} \sim^\bullet_{ie} \mathbb{E}'\{\nu x.\Box\}$, hence we have $\mathbb{E}\{\nu x.C\}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'\{\nu x.D\}$ by induction hypothesis.

  By rule LTS-RESTR we have $\nu x.R' \xrightarrow{\overline{a}} \nu x.D$, and since $\nu x.R' \sim^\circ_{ie} Q$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}'$, we have $\mathbb{E}'\{\nu x.D\} \sim^\circ_{ie} \mathbb{E}'\{C'\}$. The result then holds with rule OPEN RIGHT.

LTS-LOC. $P = a[R] \xrightarrow{\alpha} a[A]$, with $R \xrightarrow{\alpha} A$. By definition there exists R' such that $R \sim^\bullet_{ie} R'$ and $a[R'] \sim^\circ_{ie} Q$. We now distinguish three cases for A:

- A is a process T: therefore we have $R \xrightarrow{l} T$. By induction, there exists T' such that $R' \xrightarrow{l} T'$ and $T\ (\sim_{ie})^\bullet_c\ T'$. By rule LTS-LOC we have $a[R'] \xrightarrow{l} a[T']$, and since $a[R'] \sim^\circ_{ie} Q$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $a[T'] \sim^\circ_{ie} Q'$. Using CONG, we have $a[T] \sim^\bullet_{ie} a[T']$, so by OPEN RIGHT we have $a[T]\ (\sim_{ie})^\bullet_c\ Q'$ as required.

- A is an abstraction F: therefore we have $R \xrightarrow{a} F$. Let $C\ (\sim_{ie})^\bullet_c\ C'$ be closed concretions and $\mathbb{E}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'$ be closed evaluation contexts. By induction, there exists G such that $R' \xrightarrow{a} G$ and $\mathbb{E}\{a[F]\} \bullet C\ (\sim_{ie})^\bullet_c\ \mathbb{E}'\{a[G]\} \bullet C'$. By rule LTS-LOC we have $a[R'] \xrightarrow{a} a[G]$, and since $a[R'] \sim^\circ_{ie} Q$, there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}'\{a[G]\} \bullet C' \sim^\circ_{ie} \mathbb{E}'\{F'\} \bullet C'$. We have the required result by OPEN RIGHT.

- A is a concretion C: therefore we have $R \xrightarrow{\overline{a}} C$. By induction, there exists D such that $R' \xrightarrow{\overline{a}} D$ and for all $\mathbb{E}$, $\mathbb{E}'$ with $\mathbb{E}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'$, we have $\mathbb{E}\{C\}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'\{D\}$. For $\mathbb{E} \sim^\bullet_{ie} \mathbb{E}'$, we have $\mathbb{E}\{a[\Box]\} \sim^\bullet_{ie} \mathbb{E}'\{a[\Box]\}$, hence we have $\mathbb{E}\{a[C]\}\ (\sim_{ie})^\bullet_c\ \mathbb{E}'\{a[D]\}$ by induction hypothesis.

  By rule LTS-RESTR we have $a[R'] \xrightarrow{\overline{a}} a[D]$, and since $a[R'] \sim^\circ_{ie} Q$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}'$, we have $\mathbb{E}'\{a[D]\} \sim^\circ_{ie} \mathbb{E}'\{C'\}$. The result then holds with rule OPEN RIGHT.

LTS-PASSIV. $P = a[R] \xrightarrow{\overline{a}} \langle R\rangle \mathbf{0}$. By definition there exists R' such that $R \sim_{ie}^{\bullet} R'$ and $a[R'] \sim_{ie}^{\circ} Q$. By LTS-PASSIV, we have $a[R'] \xrightarrow{\overline{a}} \langle R'\rangle\mathbf{0}$, so there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $F, \mathbb{E}$, we have $F \bullet \mathbb{E}\{\langle R'\rangle\mathbf{0}\} \sim_{ie}^{\circ} F \bullet \mathbb{E}\{C'\}$, i.e. $\langle R'\rangle\mathbb{E}\{\mathbf{0}\} \sim_{ie}^{\circ} \mathbb{E}\{C'\}$.

Let $\mathbb{E}, \mathbb{E}'$ be evaluation contexts such that $\mathbb{E}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'$. We have $\mathbb{E}\{\mathbf{0}\}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'\{\mathbf{0}\}$. We also have $R\ (\sim_{ie})_c^{\bullet}\ R'$ so by CONG, we have $\langle R\rangle\mathbb{E}\{\mathbf{0}\}\ (\sim_{ie})_c^{\bullet}\ \langle R'\rangle\mathbb{E}'\{\mathbf{0}\}$. We have the required result by OPEN RIGHT.

LTS-REPLIC. $P = !R \xrightarrow{\alpha} A \mid !R$, with $R \xrightarrow{\alpha} A$. By definition there exists R' such that $R \sim_{ie}^{\bullet} R'$ and $!R' \sim_{ie}^{\circ} Q$. We now distinguish three cases for A:

- A is a process T: therefore we have $R \xrightarrow{l} T$. By induction, there exists T' such that $R' \xrightarrow{l} T'$ and $T\ (\sim_{ie})_c^{\bullet}\ T'$. By rule LTS-REPLIC we have $!R' \xrightarrow{l} T' \mid !R'$, and since $!R' \sim_{ie}^{\circ} Q$, there exists Q' such that $Q \xrightarrow{l} Q'$ and $T' \mid !R' \sim_{ie}^{\circ} Q'$. Using CONG, we have $T \mid !R \sim_{ie}^{\bullet} T' \mid !R'$, so by OPEN RIGHT we have $T \mid !R\ (\sim_{ie})_c^{\bullet}\ Q'$ as required.

- A is an abstraction F: therefore we have $R \xrightarrow{a} F$. Let $C\ (\sim_{ie})_c^{\bullet}\ C'$ be closed concretions and $\mathbb{E}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'$ be closed evaluation contexts. Since $R \sim_{ie}^{\bullet} R'$, we have $!R \sim_{ie}^{\bullet} !R'$ by CONG, hence we have $\mathbb{E}\{\Box \mid !R\}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'\{\Box \mid !R'\}$. So by induction, there exists G such that $R' \xrightarrow{a} G$ and $\mathbb{E}\{F \mid !R\} \bullet C\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'\{G \mid !R'\} \bullet C'$. By rule LTS-RESTR we have $\nu x.R' \xrightarrow{a} G \mid !R'$, and since $!R' \sim_{ie}^{\circ} Q$, there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}'\{G \mid !R'\} \bullet C' \sim_{ie}^{\circ} \mathbb{E}'\{F'\} \bullet C'$. We then have the required result by OPEN RIGHT.

- A is a concretion C: therefore we have $R \xrightarrow{\overline{a}} C$. By induction, there exists D such that $R' \xrightarrow{\overline{a}} D$ and for all $\mathbb{E}, \mathbb{E}'$ with $\mathbb{E}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'$, we have $\mathbb{E}\{C\}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'\{D\}$. For $\mathbb{E} \sim_{ie}^{\bullet} \mathbb{E}'$, we have $\mathbb{E}\{\Box \mid !R\} \sim_{ie}^{\bullet} \mathbb{E}'\{\Box \mid !R'\}$, hence we have $\mathbb{E}\{C \mid !R\}\ (\sim_{ie})_c^{\bullet}\ \mathbb{E}'\{D \mid !R'\}$ by induction hypothesis.

  By rule LTS-RESTR we have $!R' \xrightarrow{\overline{a}} D \mid !R'$, and since $!R' \sim_{ie}^{\circ} Q$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}'$, we have $\mathbb{E}'\{D \mid !R'\} \sim_{ie}^{\circ} \mathbb{E}'\{C'\}$. The result then holds with rule OPEN RIGHT.

□

With this result we can show the following lemma:

Lemma 19. *The transitive and reflexive closure of $(\sim_{ie})_c^{\bullet}$ is an input-early bisimulation.*

Proof. With property SYMM it is enough to show that $((\sim_{ie})_c^{\bullet})^*$ is a simulation. Let P, Q such that $P((\sim_{ie})_c^{\bullet})^*Q$. There exists $k \geq 0$ such that $P((\sim_{ie})_c^{\bullet})^kQ$. The proof is by induction on k. There is nothing to show for $k = 0$ since $((\sim_{ie})_c^{\bullet})^*$ is reflexive.

We suppose the result holds up to k. We have $P\ (\sim_{ie})_c^{\bullet}\ P_1 \dots P_{k-1}\ (\sim_{ie})_c^{\bullet}\ Q$ and $P \xrightarrow{a} A$. We have three cases to consider.

- A is a process P'. By induction there exists P'_{k-1} such that $P_{k-1} \xrightarrow{l} P'_{k-1}$ and $P'((\sim_{ie})^\bullet_c)^* P'_{k-1}$. By lemma 18, there exists Q' such that $Q \xrightarrow{l} Q'$ and $P'_{k-1}\ (\sim_{ie})^\bullet_c\ Q'$. We have $P'((\sim_{ie})^\bullet_c)^* Q'$ by transitivity.

- A is an abstraction F. Let C be a closed concretion and $\mathbb{E}$ be an evaluation context. By induction there exists F_{k-1} such that $P_{k-1} \xrightarrow{a} F_{k-1}$ and $\mathbb{E}\{F\} \bullet C((\sim_{ie})^\bullet_c)^* \mathbb{E}\{F_{k-1}\} \bullet C$. Since $C\ (\sim_{ie})^\bullet_c\ C$, by lemma 18, there exists F' such that $Q \xrightarrow{a} F'$ and $\mathbb{E}\{F_{k-1}\} \bullet C\ (\sim_{ie})^\bullet_c\ \mathbb{E}\{F'\} \bullet C$. We have $\mathbb{E}\{F\} \bullet C((\sim_{ie})^\bullet_c)^* \mathbb{E}\{F'\} \bullet C$ by transitivity.

- A is a concretion C. By induction there exists C_{k-1} such that $P_{k-1} \xrightarrow{\overline{a}} C_{k-1}$ and for all closed abstraction F and all closed context $\mathbb{E}$, $F \bullet \mathbb{E}\{C\}((\sim_{ie})^\bullet_c)^* F \bullet \mathbb{E}\{C_{k-1}\}$. By lemma 18, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all closed $\mathbb{E}$, we have $\mathbb{E}\{C_{k-1}\}\ (\sim_{ie})^\bullet_c\ \mathbb{E}\{C'\}$. By lemma 17, we have $F \bullet \mathbb{E}\{C_{k-1}\}\ (\sim_{ie})^\bullet_c\ F \bullet \mathbb{E}\{C'\}$. The result then holds by transitivity.

□

To prove that $\sim_{ie}$ is a congruence, it is enough to prove the following lemma:

Lemma 20. $\sim^\bullet_{ie} = \sim^\circ_{ie}$

Proof. By lemma 19 we have $(\sim_{ie})^{\bullet *}_c \subseteq \sim_{ie}$, so we have $(\sim_{ie})^{\bullet * \circ}_c \subseteq \sim^\circ_{ie}$. We now prove that $\sim^\bullet_{ie} \subseteq (\sim_{ie})^{\bullet \circ}_c$. Let P, Q such that $P \sim^\bullet_{ie} Q$. For all σ which closes P, Q, we have $P\sigma \sim^\bullet_{ie} Q\sigma$ by Subst. Since the considered processes are closed, we have $P\sigma\ (\sim_{ie})^\bullet_c\ Q\sigma$. Consequently, we have $P\ (\sim_{ie})^{\bullet \circ}_c\ Q$. Hence we have $\sim^\bullet_{ie} \subseteq (\sim_{ie})^{\bullet \circ}_c \subseteq (\sim_{ie})^{\bullet \circ *}_c \subseteq \sim^\circ_{ie}$, i.e. $\sim^\bullet_{ie} \subseteq \sim^\circ_{ie}$. The reverse inclusion is given by Open, so we have $\sim^\bullet_{ie} = \sim^\circ_{ie}$.

□

C Completeness proofs for HOπP

C.1 Strong early bisimilarity completeness

Lemma 21. *For all actions α, the relation $\xrightarrow{\alpha}$ is image-finite.*

Proof. By induction on the shape of P :

- $\mathbf{0}$: no transition from P.

- $l.Q$: one possible transition by LTS-Prefix.

- $\overline{a}\langle R\rangle Q$: one possible transition by LTS-Concr.

- $a(X)Q$: one possible transition by LTS-Abstr.

- $a[P]$: one possible transition by LTS-Passiv, and all the transitions from P (rule LTS-Loc), which are finite by induction hypothesis.

- $\nu x.P$: all the transitions from P (which are finite by induction hypothesis), minus the one labeled by x or $\overline{x}$ (rule LTS-RESTR).
- $Q \mid R$: the possible transitions are from rules LTS-FO, LTS-HO, LTS-PAR. In the case of the rule LTS-PAR, there are as many possible $\xrightarrow{\alpha}$ transitions from P as there are from Q, which are finite by induction assumption. The number of τ-transitions from P by LTS-FO (resp. LTS-HO) are bounded by the product of the number of $\xrightarrow{m}$ (resp. $\xrightarrow{a}$) transitions from Q with the number of $\xrightarrow{\overline{m}}$ (resp. $\xrightarrow{\overline{a}}$) from R, which are finite by induction assumption.
- $!P$: the possible transitions are from rule LTS-REPLIC, LTS-REPLIC-HO, LTS-REPLIC-FO. There are a finite number of $\xrightarrow{a}, \xrightarrow{\overline{a}}, \xrightarrow{m}, \xrightarrow{\overline{m}}$ transitions from P by induction, hence there are a finite number of transitions from $!P$.

□

Definition 31. *The relation $\sim_\omega$ is defined on closed processes by:*

1. $P \sim_0 Q$ *iff* $fn(P) = fn(Q)$
2. $P \sim_{k+1} Q$ *iff* $fn(P) = fn(Q)$ *and*
   - *If* $P \xrightarrow{l} P'$, *then there exists* Q' *such that* $Q \xrightarrow{l} Q'$ *and* $P' \sim_k Q'$, *and conversely if* $Q \xrightarrow{l} Q'$.
   - *If* $P \xrightarrow{a} F$, *then for all closed concretions* C, *there exists* F' *such that* $Q \xrightarrow{a} F'$ *and* $F' \bullet C \sim_k F \bullet C$, *and conversely if* $Q \xrightarrow{a} F$.
   - *If* $P \xrightarrow{\overline{a}} C$, *then for all closed abstractions* F, *there exists* C' *such that* $Q \xrightarrow{\overline{a}} C'$ *and for all closed evaluation contexts* $\mathbb{E}$, *we have* $F \bullet \mathbb{E}\{C\} \sim_k F \bullet \mathbb{E}\{C'\}$, *and conversely if* $Q \xrightarrow{\overline{a}} C$.
3. $\sim_\omega = \bigcap_k \sim_k$

Lemma 22. *The relations $\sim$ and $\sim_\omega$ coincide.*

Proof. From the definition of $\sim_\omega$, we already have that $\sim \subset \sim_\omega$. We show the converse by proving that $\sim_\omega$ is a strong bisimulation. Let P, Q be such that $P \sim_\omega Q$. We have three cases to check :

- Assume $P \xrightarrow{l} P'$. For all integers k, there exists Q_k such that $Q \xrightarrow{l} Q_k$ and $P' \sim_k Q_k$. Since $\xrightarrow{l}$ is image-finite, the set $\{Q_i | Q \xrightarrow{l} Q_i\}$ is finite. We now prove by contradiction that there exists Q' such that $Q \xrightarrow{l} Q'$ and for all k, $P' \sim_k Q'$. Assume that for all Q_i such that $Q \xrightarrow{l} Q_i$, there exists k_i such that $P' \not\sim_{k_i} Q_i$. Since $\sim_m \subset \sim_l$ if $l \leq m$, for all $m \geq k_i$, we have $P' \not\sim_m Q_i$. Since $\{Q_i | Q \xrightarrow{l} Q_i\}$ is finite, the set $\{k_i\}$ is finite and has a greatest element M. For all Q' such that $Q \xrightarrow{l} Q'$, we have $P' \not\sim_m Q'$ for all $m \geq M$. But for all k, there exists Q_k such that $Q \xrightarrow{l} Q_k$ and $P' \sim_k Q_k$, hence a contradiction. Therefore there exists Q' such that $Q \xrightarrow{l} Q'$ and for all k, $P' \sim_k Q'$, i.e. $P' \sim_\omega Q'$ as required.

- Assume $P \xrightarrow{a} F$. Let C be a closed concretion. For all k, there exists F_k such that $Q \xrightarrow{a} F_k$ and $F \bullet C \sim_k F_k \bullet C$. Since $\xrightarrow{a}$ is image-finite, the set $\{F_i | Q \xrightarrow{a} F_i\}$ is finite. By contradiction we can show that there exists F' such that $Q \xrightarrow{a} F'$ and for all k, $F' \bullet C \sim_k F \bullet C$, i.e. $F' \bullet C \sim_\omega F \bullet C$ as required.
- Assume $P \xrightarrow{\overline{a}} C$. This case is similar to the case above.

□

For the following proof we define some notations :

$$P \oplus s = \overline{s}.\mathbf{0} \mid s.P$$
$$\sum_{i=1}^{n} P_i = \nu a.(\overline{a}\langle P_1\rangle\mathbf{0} \mid \ldots \mid \overline{a}\langle P_n\rangle\mathbf{0} \mid a(X)X \mid \prod_{i=2}^{n} a(X_i)\mathbf{0})$$

We have the following properties :

- $P \oplus s \downarrow_s$
- $P \oplus s \longrightarrow P$
- For all $1 \leq i \leq n$, $\sum_{j=1}^{n} P_j \longrightarrow^n \sim P_i$

Lemma 23. *Let P, Q two closed processes. For all integers k, if $P \not\sim_k Q$ then there exists a context $\mathbb{K}$ such that $\mathbb{K}\{P\} \not\sim_b \mathbb{K}\{Q\}$.*

Proof. We proceed by induction on k. For the case $k = 0$, we must have $\mathrm{fn}(P) \neq \mathrm{fn}(Q)$. Assume we have $a \in \mathrm{fn}(P) \setminus \mathrm{fn}(Q)$ for instance. We define

$$\mathbb{K} = b[\nu a.\overline{c}\langle\square\rangle\mathbf{0} \mid R] \mid S$$
$$R = e.\mathbf{0} \mid \overline{e}.\overline{e}.d.\mathbf{0}$$
$$S = c(X)b(Y)(Y \mid Y)$$

where b, c, d, e are all distinct and do not occur in P or Q. We now prove by contradiction that $\mathbb{K}\{P\} \not\sim_b \mathbb{K}\{Q\}$. Assume that $\mathbb{K}\{P\} \sim_b \mathbb{K}\{Q\}$. We have $\mathbb{K}\{P\} \longrightarrow \nu a.(b[R] \mid b(Y)(Y \mid Y)) = T_1$ (since $a \in \mathrm{fn}(P)$ it has to be extruded during the communication). Since $\neg(T_1 \downarrow_c)$, the only way for $\mathbb{K}\{Q\}$ to match this transition is with the transition $\mathbb{K}\{Q\} \longrightarrow b[\nu a.R] \mid b(Y)(Y \mid Y) = U_1$ (we have $a \notin \mathrm{fn}(Q)$, so a is not extruded). Now we have

$$T_1 \longrightarrow \nu a.(R \mid R) = T_3$$

which can only be matched by

$$U_1 \longrightarrow (\nu a.R) \mid (\nu a.R) = U_3$$

The reduction $T_3 \longrightarrow \nu a.(e.\mathbf{0} \mid \overline{e}.\overline{e}.d.\mathbf{0} \mid \overline{e}.d.\mathbf{0}) = T_4$ can be matched by $U_3 \longrightarrow (\nu a.\overline{e}.d.\mathbf{0}) \mid (\nu a.R) = U_4$. We have $T_4 \longrightarrow \nu a.(\overline{e}.\overline{e}.d.\mathbf{0} \mid d.\mathbf{0}) = T_5$, with $T_5 \downarrow_d$: this reduction cannot be matched by U_4. Hence a contradiction.

Assume the property holds for all $k \leq n$. We now prove it for $n+1$. Since $P \sim Q$ implies $P \sim_b Q$, to prove $P_1 \not\sim_b Q_1$, it suffices to show that $P_2 \not\sim_b Q_2$ with $P_1 \sim P_2$ and $Q_1 \sim Q_2$. We distinguish the following cases :

- $P \xrightarrow{\tau} P'$. For all Q' such that $Q \xrightarrow{\tau} Q'$, we have $P' \not\sim_k Q'$. Since $\xrightarrow{\tau}$ is image-finite, the set $\{Q'_i | Q \xrightarrow{\tau} Q'_i\}$ is finite. Let N be its cardinality. By induction, there are contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{P'\} \not\sim_b \mathbb{K}_i\{Q'_i\}$ for all $i \in \{1, \ldots, N\}$. We define:

$$\mathbb{K} = a[\Box] \mid a(X) \sum_i (\mathbb{K}_i\{X\} \oplus d_i)$$

where $(d_i)_i, a$ do not occur free in P, Q. Assume that $\mathbb{K}\{P\} \sim_b \mathbb{K}\{Q\}$. Since $P \longrightarrow P'$, we have

$$\mathbb{K}\{P\} \longrightarrow a[P'] \mid a(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = R_1$$

Since $R_1 \downarrow_a$, this reduction can be matched by

$$\mathbb{K}\{Q\} \longrightarrow a[Q'_i] \mid a(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = S_1$$

for some i. We now have:

$$R_1 \longrightarrow \sum_j (\mathbb{K}_j\{P'\} \oplus d_j) = R_2$$

We have $\neg R_2 \downarrow_a$, so it can only be matched by

$$S_1 \longrightarrow \sum_j (\mathbb{K}_j\{Q'_i\} \oplus d_j) = S_2$$

Now we have $R_2 \longrightarrow^N \sim \mathbb{K}_i\{P'\} \oplus d_i = R_3$, which can only be matched by $S_2 \longrightarrow^N \sim \mathbb{K}_i\{Q'_i\} \oplus d_i = S_3$, since $R_3 \downarrow_{d_i}$. Finally we have $R_3 \longrightarrow \mathbb{K}_i\{P'\}$, which is matched by $S_3 \longrightarrow \mathbb{K}_i\{Q'_i\}$. Hence a contradiction, since $\mathbb{K}_i\{P'\} \not\sim_b \mathbb{K}_i\{Q'_i\}$, so we have $\mathbb{K}\{P\} \not\sim_b \mathbb{K}\{Q\}$ as required.

- $P \xrightarrow{m} P'$. For all Q' such that $Q \xrightarrow{m} Q'$, we have $P' \not\sim_k Q'$. Since $\xrightarrow{m}$ is image-finite, the set $\{Q'_i | Q \xrightarrow{m} Q'_i\}$ is finite. By induction, there are contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{P'\} \not\sim_b \mathbb{K}_i\{Q'_i\}$ for all i. We define:

$$\mathbb{K} = a[\Box] \mid \overline{m}.a(X) \sum_i (\mathbb{K}_i\{X\} \oplus d_i)$$

where $(d_i)_i, a$ do not occur free in P, Q. Assume that $\mathbb{K}\{P\} \sim_b \mathbb{K}\{Q\}$. We have

$$\mathbb{K}\{P\} \longrightarrow a[P'] \mid a(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = R_1$$

Since $R_1 \downarrow_a$, this reduction can be matched by

$$\mathbb{K}\{Q\} \longrightarrow a[Q'_i] \mid a(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = S_1$$

for some i. From here, this case is similar to the one above.

- $P \xrightarrow{\overline{m}} P'$. Similar to the case above.
- $P \xrightarrow{a} F$. There exists a concretion $C = \nu\widetilde{x}.\langle T\rangle U$ such that for all F' such that $Q \xrightarrow{a} F'$, we have $F' \bullet C \not\sim_k F \bullet C$. Since $\xrightarrow{a}$ is image-finite, the set $\{F'_i | Q \xrightarrow{a} F'_i\}$ is finite (let N be its cardinality). By induction, there are contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{F'_i \bullet C\} \not\sim_b \mathbb{K}_i\{F \bullet C\}$. We define:

$$\mathbb{K} = b[\Box \mid \nu\widetilde{x}.\overline{a}\langle T\rangle(U \mid \overline{e}.\mathbf{0})] \mid e.b(X) \sum_i (\mathbb{K}_i\{X\} \oplus d_i)$$

where $b, (d_i), e$ are all distinct, and do not occur free in T, U, P, Q. We have

$$\mathbb{K}\{P\} \longrightarrow b[F \bullet C \mid \overline{e}.\mathbf{0}] \mid e.b(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = R_1$$

Since $R_1 \downarrow_{\overline{e}}$, it can only be matched by a

$$\mathbb{K}\{Q\} \longrightarrow b[F'_i \bullet C \mid \overline{e}.\mathbf{0}] \mid e.b(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = S_1$$

for some i. Now we have

$$R_1 \longrightarrow b[F \bullet C] \mid b(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = R_2$$

which can only be matched by

$$S_1 \longrightarrow b[F'_i \bullet C] \mid b(X) \sum_j (\mathbb{K}_j\{X\} \oplus d_j) = S_2$$

We have then

$$R_2 \longrightarrow \sum_j (\mathbb{K}_j\{F \bullet C\} \oplus d_j) = R_3$$

which can only be matched by

$$S_2 \longrightarrow \sum_j (\mathbb{K}_j\{F'_i \bullet C\} \oplus d_j) = S_3$$

since $\neg R_3 \downarrow_b$. In turn, we have

$$R_3 \longrightarrow^N \sim \mathbb{K}_i\{F \bullet C\} \oplus d_i = R_4$$

We have $R_4 \downarrow_{d_i}$, so it can only be matched by

$$S_3 \longrightarrow^N \sim \mathbb{K}_i\{F'_i \bullet C\} \oplus d_i = S_4$$

Finally we have $R_4 \longrightarrow \mathbb{K}_i\{F \bullet C\}$, which is matched by $S_4 \longrightarrow \mathbb{K}_i\{F'_i \bullet C\}$. Hence a contradiction since by assumption we have $\mathbb{K}_i\{F \bullet C\} \not\approx_b \mathbb{K}_i\{F'_i \bullet C\}$. So we have $\mathbb{K}\{P\} \not\approx_b \mathbb{K}\{Q\}$ as required.

- $P \xrightarrow{\overline{a}} C = \nu\widetilde{x}.\langle U\rangle V$. There exists an abstraction $F = (Y)T$ such that for all C' such that $Q \xrightarrow{\overline{a}} C'$, there exists an evaluation context $\mathbb{E}$ such that $F \bullet \mathbb{E}\{C\} \not\approx_k F \bullet \mathbb{E}\{C'\}$. Since $\xrightarrow{\overline{a}}$ is finite, the set $\{C_i | Q' \xrightarrow{\overline{a}} C_i\}$ is finite (let N be its cardinality). For each i we write $\mathbb{E}_i$ the corresponding "distinguishing context". By induction, there exists contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{F \bullet \mathbb{E}_i\{C\}\} \not\approx_b \mathbb{K}_i\{F \bullet \mathbb{E}_i\{C_i\}\}$ for all i. We define

$$\mathbb{K} = b[c[\Box] \mid a(Y)(T \mid \overline{e}.\mathbf{0}) \mid c(X)\sum_i(\mathbb{E}_i\{X\}\oplus d_i)] \mid e.b(X)\sum_i(\mathbb{K}_i\{X\}\oplus d_i)$$

where $b, c, e, (d_i)$ are all distinct and do not occur free in T, P, Q. Triggering the communication on a, we have:

$$\mathbb{K}\{P\} \longrightarrow b[\nu\widetilde{x}.(c[V] \mid T\{U/Y\} \mid \overline{e}.\mathbf{0} \mid c(X)\sum_j(\mathbb{E}_j\{X\} \oplus d_j))] \mid K' = R_1$$

with $K' = e.b(X)\sum_j(\mathbb{K}_j\{X\} \oplus d_j)$. Since $R_1 \downarrow_{\overline{e}}$, it is matched for some i by

$$\mathbb{K}\{Q\} \longrightarrow b[\nu\widetilde{x}_i.(c[V_i] \mid T\{U_i/Y\} \mid \overline{e}.\mathbf{0} \mid c(X)\sum_i(\mathbb{E}_i\{X\} \oplus d_i))] \mid K' = S_1$$

with $C_i = \nu\widetilde{x}_i.\langle U_i\rangle V_i$. By triggering the passivation on c, then choosing the appropriate i in the sum, we have

$$R_1 \longrightarrow^3 \longrightarrow^N \sim b[\overline{e}.\mathbf{0} \mid F \bullet \mathbb{E}_i\{C\}] \mid K' = R_2$$

using the properties of $\oplus$ and the fact that $\sim$ is a congruence. This sequence of reduction can only be matched by

$$S_1 \longrightarrow^3 \longrightarrow^N \sim b[\overline{e}.\mathbf{0} \mid F \bullet \mathbb{E}_i\{C_i\}] \mid K' = S_2$$

From here, the proof is similar to the abstraction case. Triggering the communication on e and the passivation on b, we have

$$R_2 \longrightarrow^2 \sum_j(\mathbb{K}_j\{F \bullet \mathbb{E}_i\{C\}\} \oplus d_j) = R_3$$

which can only be matched by

$$S_2 \longrightarrow^2 \sum_j (\mathbb{K}_j\{F \bullet \mathbb{E}_i\{C_i\}\} \oplus d_j) = S_3$$

We have

$$R_3 \longrightarrow^N \sim \mathbb{K}_i\{F \bullet \mathbb{E}_i\{C\}\} \oplus d_i = R_4$$

which is matched only by

$$S_3 \longrightarrow^N \sim \mathbb{K}_i\{F \bullet \mathbb{E}_i\{C_i\}\} \oplus d_i = S_4$$

Finally we have $R_4 \longrightarrow \mathbb{K}_i\{F \bullet \mathbb{E}_i\{C\}\}$, which is matched by $S_4 \longrightarrow \mathbb{K}_i\{F \bullet \mathbb{E}_i\{C_i\}\}$. Hence a contradiction since by assumption we have $\mathbb{K}_i\{F \bullet \mathbb{E}_i\{C\}\} \not\approx_b \mathbb{K}_i\{F \bullet \mathbb{E}_i\{C_i\}\}$. So we have $\mathbb{K}\{P\} \not\approx_b \mathbb{K}\{Q\}$ as required.

□

C.2 Adaptation to strong input-early bisimilarity

We explain here how to adapt the previous proof to input-early bisimilarity. We define the slicing of $\sim_{ie}$ as follow:

Definition 32. *The relation $\sim_{ie,\omega}$ is defined on closed processes by:*

1. $P \sim_0 Q$ *iff* $fn(P) = fn(Q)$
2. $P \sim_{ie,k+1} Q$ *iff* $fn(P) = fn(Q)$ *and*
   - *If* $P \xrightarrow{l} P'$*, then there exists* Q' *such that* $Q \xrightarrow{l} Q'$ *and* $P' \sim_{ie,k} Q'$*, and conversely if* $Q \xrightarrow{l} Q'$*.*
   - *If* $P \xrightarrow{a} F$*, then for all closed concretions* C *and evaluation context* $\mathbb{E}$*, there exists* F' *such that* $Q \xrightarrow{a} F'$ *and* $\mathbb{E}\{F\} \bullet C \sim_{ie,k} \mathbb{E}\{F'\} \bullet C$*, and conversely if* $Q \xrightarrow{a} F$*.*
   - *If* $P \xrightarrow{\overline{a}} C$*, then there exists* C' *such that* $Q \xrightarrow{\overline{a}} C'$ *and for all closed abstractions* F *and all closed evaluation contexts* $\mathbb{E}$*, we have* $F \bullet \mathbb{E}\{C\} \sim_{ie,k} F \bullet \mathbb{E}\{C'\}$*, and conversely if* $Q \xrightarrow{\overline{a}} C$*.*
3. $\sim_{ie,\omega} = \bigcap_k \sim_{ie,k}$

Lemma 24. *The relation $\sim_{ie}$ and $\sim_{ie,\omega}$ coincide.*

The proof is the same as above.

Lemma 25. *Let P, Q two closed processes. For all integers k, if $P \not\sim_{ie,k} Q$ then there exists a context $\mathbb{K}$ such that $\mathbb{K}\{P\} \not\approx_b \mathbb{K}\{Q\}$.*

Proof. The proof is the same as the one of Lemma 23 except in the abstraction and concretion cases.

- $P \xrightarrow{a} F$. There exists a concretion $C = \nu\widetilde{x}.\langle T\rangle U$ and an evaluation context $\mathbb{E}$ such that for all F' such that $Q \xrightarrow{a} F'$, we have $\mathbb{E}\{F\} \bullet C \not\sim_k \mathbb{E}\{F'\} \bullet C$. Since $\xrightarrow{a}$ is image-finite, the set $\{F'_i | Q \xrightarrow{a} F'_i\}$ is finite. By induction, there are contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{\mathbb{E}\{F\} \bullet C\} \not\sim_b \mathbb{K}_i\{\mathbb{E}\{F_i\} \bullet C\}$. We define:

$$\mathbb{K} = b[\mathbb{E} \mid \nu\widetilde{x}.\overline{a}\langle T\rangle(U \mid \overline{e}.\mathbf{0})] \mid e.b(X)\sum_i(\mathbb{K}_i\{X\} \oplus d_i)$$

where $b, e, (d_i)$ are all distinct, and do not occur free in T, U, P, Q. From here the proof is similar to the early version.

- $P \xrightarrow{\overline{a}} C = \nu\widetilde{x}.\langle U\rangle V$. For all C' such that $Q \xrightarrow{\overline{a}} C'$, there exists an abstraction F and an evaluation context $\mathbb{E}$ such that $F \bullet \mathbb{E}\{C\} \not\sim_k F \bullet \mathbb{E}\{C'\}$. Since $\xrightarrow{\overline{a}}$ is finite, the set $\{C_i | Q' \xrightarrow{\overline{a}} C_i\}$ is finite (let N be its cardinality). For each i we write F_i, $\mathbb{E}_i$ the corresponding distinguishing abstraction and context. By induction, there exists contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{F_i \bullet \mathbb{E}_i\{C\}\} \not\sim_b \mathbb{K}_i\{F_i \bullet \mathbb{E}_i\{C_i\}\}$ for all i. We write $C_i = \nu\widetilde{x}_i.\langle U_i\rangle V_i$ and $F_i = (X_i)T_i$. We define

$$\mathbb{K} = b[c[\Box] \mid a(Y)(\overline{d}\langle Y\rangle\mathbf{0} \mid d(X)\sum_i(T_i\{X/X_i\} \oplus d_i) \mid K_1)] \mid K_2$$

with $K_1 = c(X)\sum_i(\mathbb{E}_i\{X\} \oplus d_i) \mid \overline{e}.\mathbf{0}$, $K_2 = e.b(X)\sum_i(\mathbb{K}_i\{X\} \oplus d_i)$, where $b, c, d, e, (d_i)$ are all distinct and do not occur free in T_i, P, Q. The main idea is to add a bogus forward on a, to enforce Q to chose a reduction. When Q has chosen a C_i, P is able to chose the corresponding index i in its sequence of reduction (here after the communication on d).

Triggering the communication on a, we have:

$$\mathbb{K}\{P\} \longrightarrow b[\nu\widetilde{x}.(c[V] \mid \overline{d}\langle U\rangle\mathbf{0} \mid d(X)\sum_j(T_j\{X/X_j\} \oplus d_j) \mid K_1)] \mid K_2 = R_2$$

Since we have $R_2 \downarrow_c$ (in K_1), it is matched for some i by

$$\mathbb{K}\{Q\} \longrightarrow b[\nu\widetilde{x}_i.(c[V_i] \mid \overline{d}\langle U_i\rangle\mathbf{0} \mid d(X)\sum_j(T_j\{X/X_j\} \oplus d_j) \mid K_1)] \mid K_2 = S_2$$

With the communication on d, we have

$$R_2 \longrightarrow b[\nu\widetilde{x}.(c[V] \mid \sum_j(T_j\{U/X_j\} \oplus d_j) \mid K_1)] \mid K_2 = R_3$$

Since we have $\neg R_3 \downarrow_d$, it is matched by

$$S_2 \longrightarrow b[\nu\widetilde{x}.(c[V] \mid \sum_j(T_j\{U_i/X_j\} \oplus d_i) \mid K_1)] \mid K_2 = S_3$$

Using properties of the sum and the fact that $\sim_{ie}$ is a congruence, we have

$$R_3 \longrightarrow^N \sim_{ie} b[\nu\widetilde{x}.(c[V] \mid T_i\{U/X_i\} \oplus d_i \mid K_1)] \mid K_2 = R_4$$

Since we have $R_4 \downarrow_{d_i}$, it is matched only by:

$$S_3 \longrightarrow^N \sim_{ie} b[\nu\widetilde{x}.(c[V] \mid T_i\{U_i/X_i\} \oplus d_i \mid K_1)] \mid K_2 = S_4$$

By property of $\oplus$, we have:

$$R_4 \longrightarrow b[\nu\widetilde{x}.(c[V] \mid T_i\{U/X_i\} \mid K_1)] \mid K_2 = R_5$$

We have $\neg R_5 \downarrow_{d_i}$, so it is matched by:

$$S_4 \longrightarrow b[\nu\widetilde{x}.(c[V] \mid T_i\{U_i/X_i\} \mid K_1)] \mid K_2 = S_5$$

From here, the proof is identical to the early version at stage R_1, S_1.

□

D Soundness proofs for HOP

We prove soundness of early context bisimilarities for HOP in the strong and weak cases. We use progress technique for the strong case and Howe's method for the weak case (it works in the strong case too).

D.1 Strong case

We have to adapt the definition 28 of progress:

Definition 33. *Let $\mathcal{R}$,$\mathcal{U}$ be binary relations on closed processes. Relation $\mathcal{R}$ is said to* strongly progress towards $\mathcal{U}$*, noted $\mathcal{R} \rightsquigarrow \mathcal{U}$ iff the following holds:*
For all closed processes such that $P \mathrel{\mathcal{R}} Q$, we have:

- *If $P \xrightarrow{l} P'$, then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathrel{\mathcal{U}} Q'$.*
- *If $P \xrightarrow{a} F$, then for all closed processes R, there exists F' such that $Q \xrightarrow{a} F'$ and $F \circ R \mathrel{\mathcal{U}} F' \circ R$.*
- *If $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S' such that $Q' \xrightarrow{\overline{a}} \langle R' \rangle S'$, $R \mathrel{\mathcal{U}} R'$ and $S \mathrel{\mathcal{U}} S'$.*

Lemma 26. *Let $\mathcal{R}$ be a reflexive binary relation on closed processes, let $\mathcal{U}$ be its reflexive and transitive closure. If $\mathcal{R} \rightsquigarrow \mathcal{U}$, then $\mathcal{U}$ is a strong simulation.*

Proof. The proof is similar to the one for Lemma 10, except in the concretion case, hence we detail this case only. With the same notations as Lemma 10, assume we have $P \xrightarrow{\overline{a}} \langle R \rangle S$. By induction, there exists R'_n, S'_n such that $P_n \xrightarrow{\overline{a}} \langle R'_n \rangle S'_n$ and $R \mathrel{\mathcal{U}} R'_n$ and $S \mathrel{\mathcal{U}} S'_n$. Since $\mathcal{R} \rightsquigarrow \mathcal{U}$ and $P_n \mathrel{\mathcal{R}} Q$, there exists R', S' such that $Q \xrightarrow{\overline{a}} \langle R' \rangle S'$ and $R_n \mathrel{\mathcal{U}} R'$ and $S_n \mathrel{\mathcal{U}} S'$. The result then holds by transitivity of $\mathcal{U}$. □

For the rest of this section, we note $\mathcal{R}=\{(P\{\widetilde{Q}/\widetilde{X}\}, P\{\widetilde{R}/\widetilde{X}\}), \text{fv}(P) = \widetilde{X}, \widetilde{Q} \dot{\sim} \widetilde{R}\}$ and its closure $\mathcal{U}=\mathcal{R}^*$. We use these relations to prove the substitution lemma. We first give some properties of these relations.

Lemma 27. *If $P \;\mathcal{U}\; Q$, then for all names a, for all closed processes T we have $P \mid T \;\mathcal{U}\; Q \mid T, a[P] \;\mathcal{U}\; a[Q], \overline{a}\langle P\rangle T \;\mathcal{U}\; \overline{a}\langle Q\rangle T, \overline{a}\langle T\rangle P \;\mathcal{U}\; \overline{a}\langle Q\rangle T, a(X)P \;\mathcal{U}\; a(X)Q, l.P \;\mathcal{U}\; l.Q, !P \;\mathcal{U} !Q, P+T \;\mathcal{U}\; Q+T$.*

Proof. We proceed by induction on n, proving that $P \;\mathcal{R}^n\; Q$ implies $P \mid T \;\mathcal{R}^n\; Q \mid T, \ldots$

For $n=1$, let $P \;\mathcal{R}\; Q$ with $P = U\{\widetilde{R}/\widetilde{X}\}$ and $Q = U\{\widetilde{S}/\widetilde{X}\}$. Since T is closed, we have $P \mid T = U\{\widetilde{R}/\widetilde{X}\} \mid T = (U \mid T)\{\widetilde{R}/\widetilde{X}\} \;\mathcal{U}\; (U \mid T)\{\widetilde{S}/\widetilde{X}\} = Q \mid T$ and $a[P] = a[U\{\widetilde{R}/\widetilde{X}\}] = a[U]\{\widetilde{R}/\widetilde{X}\} \;\mathcal{U}\; a[U]\{\widetilde{R}/\widetilde{X}\} = a[Q]$. By the same technique we have the result for the other contexts.

Assume now that the result holds up to n. We show that it holds for $n+1$. Let $P \;\mathcal{R}^{n+1}\; Q$. Then there exists P_n such that $P \;\mathcal{R}^n\; P_n \;\mathcal{R}\; Q$. By induction assumption, we have $P \mid T \;\mathcal{R}^n\; P_n \mid T$. Also we have $P_n \mid T \;\mathcal{R}\; Q \mid T$, hence we conclude $P \mid T \;\mathcal{R}^{n+1}\; Q \mid T$. We have the same for the other contexts.

□

A direct corollary from lemma 27 is if $P \;\mathcal{U}\; Q$, then for all abstractions F, we have $F \circ P \;\mathcal{U}\; F \circ Q$.

Lemma 28 (Substitution lemma)**.** *Let P be a process such that fv$(P) \subset \widetilde{X}$, and let $\widetilde{Q}$ and $\widetilde{R}$ two sets of closed processes with the same number of element than $\widetilde{X}$, and such that $\widetilde{Q} \dot{\sim} \widetilde{R}$. Then $P\{\widetilde{Q}/\widetilde{X}\} \dot{\sim} P\{\widetilde{R}/\widetilde{X}\}$.*

Proof. We show that the transitive and reflexive closure $\mathcal{U}$ of $\mathcal{R}$ is a strong simulation. As $\mathcal{U}$ is symmetrical, it will imply that $\mathcal{U}$ is a strong bisimulation. By lemma 26, it suffices to show that $\mathcal{R} \leadsto \mathcal{U}$.

For all process P such that fv$(P) = \widetilde{X}$ and for all closed processes $\widetilde{R}$ with the same number of elements than $\widetilde{X}$, we write P_R for $P\{\widetilde{R}/\widetilde{X}\}$.

We proceed by induction on the derivation $P_Q \xrightarrow{\alpha} A_Q$. A common subcase is the case $P = X$, and the derivation comes from Q. In this case, we have $P_Q = Q, P_R = R$ with $Q \dot{\sim} R$. Since $\dot{\sim} \subseteq \mathcal{R} \subseteq \mathcal{U}$, we have $Q \;\mathcal{U}\; R$. Therefore we consider $P \neq X$ in the following cases.

LTS-Prefix. In this case, we have $P_Q = l.S_Q$. So $P_R = l.S_R$ and $P_R \xrightarrow{l} S_R$. We have $S_Q \;\mathcal{R}\; S_R$, so we have $S_Q \;\mathcal{U}\; S_R$ as required.

LTS-Abstr. In this case, we have $P_Q = a(X)S_Q$, and A_Q is an abstraction $F_Q = (X)S_Q$. Then $P_R = a(X)S_R$. Let T be a closed process. We have $P_R \xrightarrow{a} F_R$. Since T is closed, we have $F_Q \circ T = (F \circ T)_Q \;\mathcal{R}\; (F \circ T)_R = F_R \circ T$. Hence we have $F_Q \circ T \;\mathcal{U}\; F_R \circ T$ as required.

LTS-Concr. In this case, we have $P_Q = \overline{a}\langle S_Q\rangle T_Q$, and $P_Q \xrightarrow{\overline{a}} \langle S_Q\rangle T_Q = C_Q$. Hence $P_R = \overline{a}\langle S_R\rangle T_R$. We have $P_R \xrightarrow{\overline{a}} C_R$, and $S_Q \;\mathcal{R}\; S_R, T_Q \;\mathcal{R}\; T_R$, hence the result holds.

LTS-FO. In this case, we have $P_Q = S_Q \mid T_Q$ with $S_Q \xrightarrow{m} U_Q$, $T_Q \xrightarrow{\overline{m}} V_Q$. So $P_Q \xrightarrow{\tau} U_Q \mid V_Q$.

By induction, there exists U'_R such that $S_R \xrightarrow{m} U'_R$ and $U_Q \;\mathcal{U}\; U'_R$, and there exists V'_R such that $T_R \xrightarrow{\overline{m}} V'_R$ and $V_Q \;\mathcal{U}\; V'_R$. By LTS-FO we have $S_R \mid T_R \xrightarrow{\tau} U'_R \mid V'_R$. By lemma 27, we have $U_Q \mid V_Q \;\mathcal{U}\; U'_R \mid V_Q \;\mathcal{U}\; U'_R \mid V'_R$, so by transitivity we have $U_Q \mid V_Q \;\mathcal{U}\; U'_R \mid V'_R$, as required.

LTS-Replic-FO. Similar to he case above.

LTS-HO. In this case, we have $P_Q = S_Q \mid T_Q$ with $S_Q \xrightarrow{a} F$, $T_Q \xrightarrow{\overline{a}} C = \langle V \rangle W$, and $P_Q \xrightarrow{\tau} F \bullet C$.

By induction, there exists U' such that $S_R \xrightarrow{a} F'$ and $F \circ V \;\mathcal{U}\; F' \circ V$, and there exists $C' = \langle V' \rangle W'$ such that $T_R \xrightarrow{\overline{a}} C'$ and $V \;\mathcal{U}\; V', W \;\mathcal{U}\; W'$. By LTS-HO we have $S_R \mid T_R \xrightarrow{\tau} F' \bullet C'$. By lemma 27, we have $F \bullet C \;\mathcal{U}\; F' \circ V' \mid W$. Since $W \;\mathcal{U}\; W'$, we have $F' \circ V' \mid W \;\mathcal{U}\; F' \circ V' \mid W' = F' \bullet C'$, so by transitivity we have $F \bullet C \;\mathcal{U}\; F' \bullet C'$ as required.

LTS-Replic-HO. Similar to the case above (with one additional use of the lemma 27)

LTS-Par. In this case, we have $P_Q = S_Q \mid T_Q$, $A_Q = B_Q \mid T_Q$ with $S_Q \xrightarrow{\alpha} B_Q$. We have to discuss on the shape of B_Q:

- B_Q is a process U: then $S_Q \xrightarrow{l} U$. So by induction, there exists U' such that $S_R \xrightarrow{l} U'$ and $U \;\mathcal{U}\; U'$. By rule LTS-Par, we have $P_R \xrightarrow{l} U' \mid T_R$, and by lemma 27, we have $U \mid T_Q \;\mathcal{U}\; U' \mid T_Q$. As $T_Q \;\mathcal{U}\; T_R$, we have $U' \mid T_Q \;\mathcal{U}\; U' \mid T_R$ by lemma 27. Finally we have $P_R \xrightarrow{l} U' \mid T_R$ and by transitivity of $\mathcal{U}$, we have $U \mid T_Q \;\mathcal{U}\; U' \mid T_R$ as required.
- B_Q is an abstraction F: then $S_Q \xrightarrow{a} F$. Let V be a closed process. By induction, there exists F' such that $S_R \xrightarrow{a} F'$ and $F \circ V \;\mathcal{U}\; F' \circ V$. By LTS-Par, we have $P_R \xrightarrow{a} F' \mid T_R$. By lemma 27, we have $(F \mid T_Q) \circ V \;\mathcal{U}\; F' \circ V \mid T_Q$ and since $T_Q \;\mathcal{R}\; T_R$, we have $F' \circ V \mid T_Q \;\mathcal{U}\; F' \circ V \mid T_R = (F' \mid T_R) \circ V$. Hence by transitivity of $\mathcal{U}$, we have $(F \mid T_Q) \circ V \;\mathcal{U}\; (F' \mid T_R) \circ V$ as required.
- B_Q is a concretion $C = \langle U \rangle V$. By induction, there exists $C' = \langle U' \rangle V'$ such that $S_R \xrightarrow{\overline{a}} C'$ and $U \;\mathcal{U}\; U', V \;\mathcal{U}\; V'$. Since $V \;\mathcal{U}\; V'$, by lemma 27, we have $V \mid T_Q \;\mathcal{U}\; V' \mid T_Q$, and from $T_Q \;\mathcal{U}\; T_R$ we have $V' \mid T_Q \;\mathcal{U}\; V' \mid T_R$. By transitivity, we have $V \mid T_Q \;\mathcal{U}\; V' \mid T_R$ as required.

LTS-Loc. In this case, we have $P_Q = a[S_Q]$ with $S_Q \xrightarrow{\alpha} B_Q$. We have three cases to consider:

- B_Q is a process U: we have $S_Q \xrightarrow{l} U$. By induction there exists U' such that $S_R \xrightarrow{l} U'$ and $U \;\mathcal{U}\; U'$. By LTS-Loc we have $P_R \xrightarrow{l} a[U']$ and by lemma 27 we have $a[U] \;\mathcal{U}\; a[U']$ as required.

- B_Q is an abstraction F: we have $S_Q \xrightarrow{b} F$. Let V be a closed process. By induction there exists F' such that $S_R \xrightarrow{b} F'$ and $F \circ V \,\mathcal{U}\, F' \circ V$. By LTS-Loc, we have $P_R \xrightarrow{b} a[F']$. By lemma 27, we have $a[F] \circ V = a[F \circ V] \,\mathcal{U}\, a[F' \circ V] = a[F'] \circ V$, hence the result holds.

- B_Q is a concretion $C = \langle U \rangle V$: then $S_Q \xrightarrow{\overline{b}} C$. By induction, there exists $C' = \langle U' \rangle V'$ such that $S_R \xrightarrow{\overline{b}} C'$ and $U \,\mathcal{U}\, U', V \,\mathcal{U}\, V'$. We have $P_R \xrightarrow{\overline{b}} a[C']$ by LTS-Loc, and by lemma 27, we have $a[V] \,\mathcal{U}\, a[V']$ as required.

LTS-Passiv. In this case, we have $P_Q = a[S_Q]$ and $P_Q \xrightarrow{\overline{a}} \langle S_Q \rangle \mathbf{0}$. We have $P_R \xrightarrow{\overline{a}} \langle S_R \rangle \mathbf{0}$, and we have $S_Q \,\mathcal{R}\, S_R$ and $\mathbf{0} \,\mathcal{R}\, \mathbf{0}$, hence the result holds.

LTS-Replic. In this case, we have $P_Q = !S_Q$ with $S_Q \xrightarrow{\alpha} A_Q$ and $P_Q \xrightarrow{\alpha} A_Q \mid P_Q$. We have three cases to consider:

- A_Q is a process T: we have $S_Q \xrightarrow{l} T$. By induction there exists T' such that $S_R \xrightarrow{l} T'$ and $T \,\mathcal{U}\, T'$. By LTS-Replic we have $P_R \xrightarrow{l} T' \mid !S_R$. By lemma 27, we have $T \mid P_Q \,\mathcal{U}\, T' \mid P_Q \,\mathcal{U}\, T' \mid P_R$ (since $P_Q \,\mathcal{U}\, P_R$). We have the result by transitivity.

- B_Q is an abstraction F: we have $S_Q \xrightarrow{b} F$. Let V be a closed process. By induction there exists F' such that $S_R \xrightarrow{b} F'$ and $F \circ V \,\mathcal{U}\, F' \circ V$. By LTS-Replic, we have $P_R \xrightarrow{b} F' \mid !S_R$. By lemma 27, we have $(F \mid P_Q) \circ V = F \circ V \mid P_Q \,\mathcal{U}\, F' \circ V \mid P_Q$ and $F' \circ V \mid P_Q \,\mathcal{U}\, F' \circ V \mid P_R = (F' \mid P_R) \circ V$, hence the result holds by transitivity.

- B_Q is a concretion $C = \langle U \rangle V$: then $S_Q \xrightarrow{\overline{b}} C$. By induction, there exists $C' = \langle U' \rangle V'$ such that $S_R \xrightarrow{\overline{b}} C'$ and $U \,\mathcal{U}\, U', V \,\mathcal{U}\, V'$. We have $P_R \xrightarrow{\overline{b}} C' \mid P_R$ by LTS-Loc, and by lemma 27 we have $P_Q \mid V \,\mathcal{U}\, P_R \mid V$ and $P_R \mid V \,\mathcal{U}\, P_R \mid V'$, hence the result holds by transitivity.

LTS-Sum. In this case, we have $P_Q = S_Q + T_Q$, $A_Q = B_Q$ with $S_Q \xrightarrow{\alpha} B_Q$. We have to discuss on the shape of B_Q:

- B_Q is a process U: then $S_Q \xrightarrow{l} U$. So by induction, there exists U' such that $S_R \xrightarrow{l} U'$ and $U \,\mathcal{U}\, U'$. By rule LTS-Sum, we have $P_R \xrightarrow{l} U'$, hence the result holds.

- B_Q is an abstraction F: then $S_Q \xrightarrow{a} F$. Let V be a closed process. By induction, there exists F' such that $S_R \xrightarrow{a} F'$ and $F \circ V \,\mathcal{U}\, F' \circ V$. By LTS-Sum, we have $P_R \xrightarrow{a} F'$, hence the result holds.

$$X \mathrel{\overset{\wedge}{\mathcal{R}}} X \qquad \mathbf{0} \mathrel{\overset{\wedge}{\mathcal{R}}} \mathbf{0} \qquad \frac{P \mathrel{\mathcal{R}} Q}{l.P \mathrel{\overset{\wedge}{\mathcal{R}}} l.Q} \qquad \frac{P \mathrel{\mathcal{R}} Q}{\nu x.P \mathrel{\overset{\wedge}{\mathcal{R}}} \nu x.Q} \qquad \frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{P_1 \mid P_2 \mathrel{\overset{\wedge}{\mathcal{R}}} Q_1 \mid Q_2}$$

$$\frac{P \mathrel{\mathcal{R}} Q}{a(X)P \mathrel{\overset{\wedge}{\mathcal{R}}} a(X)Q} \qquad \frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{\overline{a}\langle P_1 \rangle P_2 \mathrel{\overset{\wedge}{\mathcal{R}}} \overline{a}\langle Q_1 \rangle Q_2} \qquad \frac{P \mathrel{\mathcal{R}} Q}{a[P] \mathrel{\overset{\wedge}{\mathcal{R}}} a[Q]}$$

$$\frac{P_1 \mathrel{\mathcal{R}} Q_1 \qquad P_2 \mathrel{\mathcal{R}} Q_2}{P_1 + P_2 \mathrel{\overset{\wedge}{\mathcal{R}}} Q_1 + Q_2} \qquad \frac{P \mathrel{\mathcal{R}} Q}{!P \mathrel{\overset{\wedge}{\mathcal{R}}} !Q}$$

Figure 8: Compatible refinement for HOP processes

- B_Q is a concretion $C = \langle U \rangle V$. By induction, there exists $C' = \langle U' \rangle V'$ such that $S_R \xrightarrow{\overline{a}} C'$ and $U \mathrel{\mathcal{U}} U', V \mathrel{\mathcal{U}} V'$. By LTS-SUM, we have $P_R \xrightarrow{a} C'$, hence the result holds.

□

From the substitution lemma, we have directly the theorem:

Theorem 11. *If $Q \dot{\sim} R$ then for all a, l, T, we have $Q \mid T \dot{\sim} R \mid T$, $a[Q] \dot{\sim} a[R]$, $a(Y)Q \dot{\sim} a(Y)R$, $\overline{a}\langle Q \rangle T \dot{\sim} \overline{a}\langle R \rangle T$, $\overline{a}\langle T \rangle Q \dot{\sim} \overline{a}\langle T \rangle R$, $l.Q \dot{\sim} l.R$, $Q + T \dot{\sim} R + T$, $!Q \dot{\sim} !R$.*

D.2 Weak case

In the proofs, we use the following property:

Lemma 29. *If $P \dot{\approx}^{\circ} Q$ then:*

- *If $P \overset{l}{\Rightarrow} P'$, then there exists Q' such that $Q \overset{l}{\Rightarrow} Q'$ and $P' \dot{\approx}^{\circ} Q'$.*
- *If $P \overset{a}{\Rightarrow} F$, for all R, there exists F', Q' such that $Q \overset{a}{\Rightarrow} F'$, $F' \circ R \overset{\tau}{\Rightarrow} Q'$, and $F \circ R \dot{\approx}^{\circ} Q'$*
- *If $P \overset{\overline{a}}{\Rightarrow} \langle R \rangle S$, there exists R', S', S'' such that $Q \overset{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \overset{\tau}{\Rightarrow} S'$, $R \dot{\approx}^{\circ} R'$, and $S \dot{\approx}^{\circ} S'$.*

Proof. By induction on $P \overset{\alpha}{\Rightarrow} A$ □

The compatible refinement for HOP is given Fig. 8. The Howe's closure definition and properties (Lemma 15) can be found in Appendix B.

Lemma 30. *Let $(\dot{\approx})^{\bullet}_{c}$ be the restriction of $\dot{\approx}^{\bullet}$ to closed terms. If $P\ (\dot{\approx})^{\bullet}_{c}\ Q$ then :*

- *If $P \xrightarrow{l} P'$, there exists Q' such that $Q \overset{l}{\Rightarrow} Q'$ and $P'\ (\dot{\approx})^{\bullet}_{c}\ Q'$.*

- *If $P \xrightarrow{a} F$, for all closed processes $T \ (\dot{\approx})^{\bullet}_{c}\ T'$, there exists F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ T' \stackrel{\tau}{\Rightarrow} Q'$, and $F \circ T \ (\dot{\approx})^{\bullet}_{c}\ Q'$*
- *If $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S', S'' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \stackrel{\tau}{\Rightarrow} S'$, $R \ (\dot{\approx})^{\bullet}_{c}\ R'$, and $S \ (\dot{\approx})^{\bullet}_{c}\ S'$.*

Proof. Let P, Q be processes such that $P \ (\dot{\approx})^{\bullet}_{c}\ Q$ and $P \xrightarrow{\alpha} A$. We proceed by induction on the derivation $P \xrightarrow{\alpha} A$. As pointed out in the proof of Lemma 18 (Appendix B), we suppose that the intermediate processes introduced by Howe's closure definition are closed. We also work with $\dot{\approx}^{\circ}$ instead of $\approx$ when all the processes are closed.

LTS-Prefix. $P = l.P' \xrightarrow{l} P'$. By definition there exists R such that $P' \ \dot{\approx}^{\bullet}\ R$ and $l.R \ \dot{\approx}^{\circ}\ Q$. By LTS-Prefix we have $l.R \xrightarrow{l} R$, so there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and $R \ \dot{\approx}^{\circ}\ Q'$. By Open right we have $P' \ \dot{\approx}^{\bullet}\ Q'$, and since P' and Q' are closed, we have $P' \ (\dot{\approx})^{\bullet}_{c}\ Q'$ as required.

LTS-Abstr. $P = a(X)P' \xrightarrow{a} (X)P'$. By definition there exists R such that $P' \ \dot{\approx}^{\bullet}\ R$ and $a(X)R \ \dot{\approx}^{\circ}\ Q$. Let $T \ (\dot{\approx})^{\bullet}_{c}\ T'$ be closed processes. By LTS-Abstr we have $a(X)R \xrightarrow{a} (X)R$, so by bisimilarity there exists F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ T' \stackrel{\tau}{\Rightarrow} Q'$, and $(X)R \circ T' \ \dot{\approx}^{\circ}\ Q'$.

We have $P' \ \dot{\approx}^{\bullet}\ R$ and $T \ \dot{\approx}^{\bullet}\ T'$, so by Subst we have $(X)P' \circ T \ (\dot{\approx})^{\bullet}_{c}\ (X)R \circ T'$. By Open right, we have $(X)P' \circ T \ (\dot{\approx})^{\bullet}_{c}\ Q'$ as required.

LTS-Concr. $P = \overline{a}\langle R \rangle S \xrightarrow{\overline{a}} \langle R \rangle S$. By definition there exists T, U such that $R \ \dot{\approx}^{\bullet}\ T$, $S \ \dot{\approx}^{\bullet}\ U$ and $\overline{a}\langle T \rangle U \ \dot{\approx}^{\circ}\ Q$. By LTS-Concr we have $\overline{a}\langle T \rangle U \xrightarrow{\overline{a}} \langle T \rangle U$, so there exists R', S', S'' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \stackrel{\tau}{\Rightarrow} S'$, $T \ \dot{\approx}^{\circ}\ R'$, and $U \ \dot{\approx}^{\circ}\ S'$. We have $R \ (\dot{\approx})^{\bullet}_{c}\ R'$ and $S \ (\dot{\approx})^{\bullet}_{c}\ S'$ using Open right.

LTS-Par. $P = U \mid V \xrightarrow{\alpha} A \mid V$ with $U \xrightarrow{\alpha} A$. By definition there exists U', V' such that $U \ \dot{\approx}^{\bullet}\ U'$, $V \ \dot{\approx}^{\bullet}\ V'$ and $U' \mid V' \ \dot{\approx}^{\circ}\ Q$. We have three cases to consider for A:

- A is a process T: therefore we have $U \xrightarrow{l} T$. By induction, there exists T' such that $U' \stackrel{l}{\Rightarrow} T'$ and $T \ (\dot{\approx})^{\bullet}_{c}\ T'$. Using Cong, we have $T \mid V \ \dot{\approx}^{\bullet}\ T' \mid V'$. By several applications of rule LTS-Par we have $U' \mid V' \stackrel{l}{\Rightarrow} T' \mid V'$, and since $U' \mid V' \ \dot{\approx}^{\circ}\ Q$, there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and $T' \mid V' \ \dot{\approx}^{\circ}\ Q'$. We have $T \mid V \ (\dot{\approx})^{\bullet}_{c}\ Q'$ by Open right.
- A is an abstraction F: therefore we have $U \xrightarrow{a} F$. Let $T \ (\dot{\approx})^{\bullet}_{c}\ T'$ be closed processes. By induction, there exists G, U'' such that $U' \stackrel{a}{\Rightarrow} G$, $G \circ T \stackrel{\tau}{\Rightarrow} U''$, and $F \circ T \ (\dot{\approx})^{\bullet}_{c}\ U''$. By Cong, we have $(F \mid V) \circ T \ (\dot{\approx})^{\bullet}_{c}\ U'' \mid V'$.

  By several application of rule LTS-Par, we have $U' \mid V' \stackrel{a}{\Rightarrow} G \mid V'$, and since $U' \mid V' \ \dot{\approx}^{\circ}\ Q$, there exists F', Q'' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ T' \stackrel{\tau}{\Rightarrow} Q''$, and $(G \mid V') \circ T' \ \dot{\approx}^{\circ}\ Q''$. Since $G \circ T' \stackrel{\tau}{\Rightarrow} U''$, we have $(G \mid V') \circ T' \stackrel{\tau}{\Rightarrow}$

$U'' \mid V'$ by LTS-PAR. We have $(G \mid S') \circ T' \dot{\approx}^\circ Q''$, so there exists Q' such that $Q'' \stackrel{\tau}{\Rightarrow} Q'$ and $U'' \mid V' \dot{\approx}^\circ Q'$. We then have $(F \mid V) \circ T \ (\dot{\approx})^\bullet_c \ Q'$ by OPEN RIGHT.

- A is a concretion $\langle R \rangle S$: therefore we have $U \xrightarrow{\overline{a}} \langle R \rangle S$. By induction, there exists $\langle R'' \rangle U''$, S'' such that $U' \stackrel{\overline{a}}{\Rightarrow} \langle R'' \rangle U''$, $U'' \stackrel{\tau}{\Rightarrow} S''$, $R \ (\dot{\approx})^\bullet_c \ R''$, and $S \ (\dot{\approx})^\bullet_c \ S''$. By CONG, we have $S \mid V \ (\dot{\approx})^\bullet_c \ S'' \mid V'$.

  By several application of rule LTS-PAR we have $U' \mid V' \stackrel{\overline{a}}{\Rightarrow} \langle R'' \rangle U'' \mid V'$, and since we have $U' \mid V' \dot{\approx}^\circ Q$, there exists $\langle R' \rangle Q'$ such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle Q'$, $R'' \dot{\approx}^\circ R'$, and $U'' \mid V' \dot{\approx}^\circ Q'$. By LTS-PAR, we have $U'' \mid V' \stackrel{\tau}{\Rightarrow} S'' \mid V'$, so there exists S' such that $Q' \xrightarrow{\tau} S'$ and $S'' \mid V' \dot{\approx}^\circ S'$. Finally we have $R \ (\dot{\approx})^\bullet_c \ R'$ and $S \mid V \ (\dot{\approx})^\bullet_c \ S'$ by OPEN RIGHT.

LTS-FO. $P = R \mid S \xrightarrow{\tau} U \mid V$ with $R \xrightarrow{m} U$ and $S \xrightarrow{\overline{m}} V$ for some m. By definition there exists R', S' such that $R \dot{\approx}^\bullet R'$, $S \dot{\approx}^\bullet S'$ and $R' \mid S' \dot{\approx}^\circ Q$. By induction, there exists U', V' such that $R' \stackrel{m}{\Rightarrow} U'$ and $S' \stackrel{\overline{m}}{\Rightarrow} V'$ such that $U \ (\dot{\approx})^\bullet_c \ U'$ and $V \ (\dot{\approx})^\bullet_c \ V'$. By LTS-FO and rule LTS-PAR to handle τ steps, we have $R' \mid S' \stackrel{\tau}{\Rightarrow} U' \mid V'$. Since $R' \mid S' \dot{\approx}^\circ Q$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $U' \mid V' \dot{\approx}^\circ Q'$.

We have $U \ (\dot{\approx})^\bullet_c \ U'$ and $V \ (\dot{\approx})^\bullet_c \ V'$, so by CONG, we have $U \mid V \dot{\approx}^\bullet U' \mid V'$. By OPEN RIGHT we have $U \mid V \ (\dot{\approx})^\bullet_c \ Q'$ as required.

LTS-REPLIC-FO Similar to the case above.

LTS-HO. $P = U \mid V \xrightarrow{\tau} F \bullet \langle R \rangle S$, with $U \xrightarrow{a} F$ and $V \xrightarrow{\overline{a}} \langle R \rangle S$ for some a. By definition there exists U', V' such that $U \dot{\approx}^\bullet U'$, $V \dot{\approx}^\bullet V'$ and $U' \mid V' \dot{\approx}^\circ Q$.

By induction, there exists $\langle R' \rangle S''$, S' such that $V' \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \stackrel{\tau}{\Rightarrow} S'$, $R \ (\dot{\approx})^\bullet_c \ R'$, and $S \ (\dot{\approx})^\bullet_c \ S'$. Since we have $R \ (\dot{\approx})^\bullet_c \ R'$, there exists F', U'' such that $U' \stackrel{a}{\Rightarrow} F'$, $F' \circ R' \stackrel{\tau}{\Rightarrow} U''$, and $F \circ R \ (\dot{\approx})^\bullet_c \ U''$. Since $S \ (\dot{\approx})^\bullet_c \ S'$, we have $F \bullet \langle R \rangle S \ (\dot{\approx})^\bullet_c \ U'' \mid S'$ by CONG.

By rule LTS-HO and rule LTS-PAR to handle τ steps, we have $U' \mid V' \stackrel{\tau}{\Rightarrow} F' \bullet \langle R' \rangle S''$. Since $F' \circ R' \stackrel{\tau}{\Rightarrow} U''$ and $S'' \stackrel{\tau}{\Rightarrow} S'$, we have $F' \bullet \langle R' \rangle S'' \stackrel{\tau}{\Rightarrow} U'' \mid S'$ by LTS-PAR. From $U' \mid V' \dot{\approx}^\circ Q$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $U'' \mid S' \dot{\approx}^\circ Q'$. Finally, we have the required result by OPEN RIGHT.

LTS-REPLIC-HO Similar to the case above.

LTS-LOC. $P = a[U] \xrightarrow{\alpha} a[A]$ with $U \xrightarrow{\alpha} A$. By definition there exists U' such that $U \dot{\approx}^\bullet U'$ and $a[U'] \dot{\approx}^\circ Q$. We have three cases to consider for A:

- A is a process T: therefore we have $U \xrightarrow{l} T$. By induction, there exists T' such that $U' \stackrel{l}{\Rightarrow} T'$ and $T \ (\dot{\approx})^\bullet_c \ T'$. By several applications of rule LTS-LOC we have $a[U'] \stackrel{l}{\Rightarrow} a[T']$, and since $a[U'] \dot{\approx}^\circ Q$, there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and $a[T'] \dot{\approx}^\circ Q'$. Using CONG, we have $a[T] \dot{\approx}^\bullet a[T']$, so by OPEN RIGHT we have $a[T] \ (\dot{\approx})^\bullet_c \ Q'$ as required.

- A is an abstraction F: therefore we have $U \xrightarrow{b} F$. Let $T\ (\dot{\approx})^{\bullet}_{c}\ T'$ be closed processes. By induction, there exists G, U'' such that $U' \overset{b}{\Rightarrow} G$, $G \circ T' \overset{\tau}{\Rightarrow} U''$, and $F \circ T\ (\dot{\approx})^{\bullet}_{c}\ U''$. By CONG, we have $a[F] \circ T\ (\dot{\approx})^{\bullet}_{c}\ a[U'']$.

  By several application of rule LTS-LOC, we have $a[U'] \overset{b}{\Rightarrow} a[G]$, and since $a[U'] \dot{\approx}^{\circ} Q$, there exists F', Q'' such that $Q \overset{b}{\Rightarrow} F'$, $F' \circ T' \overset{\tau}{\Rightarrow} Q''$, and $a[G] \circ T' \dot{\approx}^{\circ} Q''$. We have $a[G] \circ T' \overset{\tau}{\Rightarrow} a[U'']$, hence there exists Q' such that $Q'' \overset{\tau}{\Rightarrow} Q'$ and $a[U''] \dot{\approx}^{\circ} Q'$. We then have $a[F] \circ T\ (\dot{\approx})^{\bullet}_{c}\ Q'$ by OPEN RIGHT.

- A is a concretion $\langle R \rangle S$: therefore we have $U \xrightarrow{\bar{b}} \langle R \rangle S$. By induction, there exists $\langle R'' \rangle U''$, S'' such that $U' \overset{\bar{b}}{\Rightarrow} \langle R'' \rangle U''$, $U'' \overset{\tau}{\Rightarrow} S''$, $R\ (\dot{\approx})^{\bullet}_{c}\ R''$, and $S\ (\dot{\approx})^{\bullet}_{c}\ S''$. By CONG, we have $a[S]\ (\dot{\approx})^{\bullet}_{c}\ a[S'']$.

  By several application of rule LTS-LOC we have $a[U'] \overset{\bar{b}}{\Rightarrow} \langle R'' \rangle a[U'']$, and since we have $a[U'] \dot{\approx}^{\circ} Q$, there exists $\langle R' \rangle Q''$, Q' such that $Q \overset{\bar{a}}{\Rightarrow} \langle R' \rangle Q''$, $Q'' \overset{\tau}{\Rightarrow} Q'$, $R'' \dot{\approx}^{\circ} R'$, and $a[U''] \dot{\approx}^{\circ} Q'$. We have $a[U''] \overset{\tau}{\Rightarrow} a[S'']$, hence there exists S' such that $Q' \overset{\tau}{\Rightarrow} S'$ and $a[S''] \dot{\approx}^{\circ} S'$. Finally we have $R\ (\dot{\approx})^{\bullet}_{c}\ R'$ and $a[S]\ (\dot{\approx})^{\bullet}_{c}\ S'$ by OPEN RIGHT.

LTS-PASSIV. $P = a[R] \xrightarrow{\bar{a}} \langle R \rangle \mathbf{0}$. By definition there exists T such that $R \dot{\approx}^{\bullet} T$ and $a[T] \dot{\approx}^{\circ} Q$. By LTS-PASSIV we have $a[T] \xrightarrow{\bar{a}} \langle T \rangle \mathbf{0}$, so there exists R', S', S'' such that $Q \overset{\bar{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \overset{\tau}{\Rightarrow} S'$, $T \dot{\approx}^{\circ} R'$, and $\mathbf{0} \dot{\approx}^{\circ} S'$. We have $R\ (\dot{\approx})^{\bullet}_{c}\ R'$ and $\mathbf{0}\ (\dot{\approx})^{\bullet}_{c}\ S'$ using OPEN RIGHT and reflexivity.

LTS-SUM. $P = U + V \xrightarrow{\alpha} A$ with $U \xrightarrow{\alpha} A$. By definition there exists U', V' such that $U \dot{\approx}^{\bullet} U'$, $V \dot{\approx}^{\bullet} V'$ and $U' + V' \dot{\approx}^{\circ} Q$. We have three cases to consider for A:

- A is a process T: therefore we have $U \xrightarrow{l} T$. By induction, there exists T' such that $U' \overset{l}{\Rightarrow} T'$ and $T\ (\dot{\approx})^{\bullet}_{c}\ T'$. By rule LTS-SUM we have $U' + V' \overset{l}{\Rightarrow} T'$, and since $U' + V' \dot{\approx}^{\circ} Q$, there exists Q' such that $Q \overset{l}{\Rightarrow} Q'$ and $T' \dot{\approx}^{\circ} Q'$. We have the required result by OPEN RIGHT.

- A is an abstraction F: therefore we have $U \xrightarrow{a} F$. Let $T\ (\dot{\approx})^{\bullet}_{c}\ T'$ be closed processes. By induction, there exists G, U'' such that $U' \overset{b}{\Rightarrow} G$, $G \circ T' \overset{\tau}{\Rightarrow} U''$, and $F \circ T\ (\dot{\approx})^{\bullet}_{c}\ U''$.

  By LTS-SUM, we have $U' + V' \overset{a}{\Rightarrow} G$, and since $U' + V' \dot{\approx}^{\circ} Q$, there exists F', Q'' such that $Q \overset{a}{\Rightarrow} F'$, $F' \circ T' \overset{\tau}{\Rightarrow} Q''$, and $G \circ T' \dot{\approx}^{\circ} Q''$. We have $G \circ T' \overset{\tau}{\Rightarrow} U''$, hence there exists Q' such that $Q'' \overset{\tau}{\Rightarrow} Q'$ and $U'' \dot{\approx}^{\circ} Q'$. We then have $F \circ T\ (\dot{\approx})^{\bullet}_{c}\ Q'$ by OPEN RIGHT.

- A is a concretion $\langle R \rangle S$: therefore we have $U \xrightarrow{\bar{a}} \langle R \rangle S$. By induction, there exists $\langle R'' \rangle U''$, S'' such that $U' \overset{\bar{a}}{\Rightarrow} \langle R'' \rangle U''$, $U'' \overset{\tau}{\Rightarrow} S''$, $R\ (\dot{\approx})^{\bullet}_{c}\ R''$, and $S\ (\dot{\approx})^{\bullet}_{c}\ S''$.

By LTS-SUM we have $U'+V' \stackrel{\overline{a}}{\Rightarrow} \langle R''\rangle U''$, and since we have $U'+V' \mathrel{\dot{\approx}^\circ} Q$, there exists $\langle R'\rangle Q''$, Q' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R'\rangle Q''$, $Q'' \stackrel{\tau}{\Rightarrow} Q'$, $R'' \mathrel{\dot{\approx}^\circ} R'$, and $U'' \mathrel{\dot{\approx}^\circ} Q'$. We have $U'' \stackrel{\tau}{\Rightarrow} S''$, hence there exists S' such that $Q' \stackrel{\tau}{\Rightarrow} S'$ and $S'' \mathrel{\dot{\approx}^\circ} S'$. Finally we have $R\ (\dot{\approx})^\bullet_c\ R'$ and $S\ (\dot{\approx})^\bullet_c\ S'$ by OPEN RIGHT.

LTS-REPLIC. $P = !U \xrightarrow{\alpha} A \mid !U$ with $U \xrightarrow{\alpha} A$. By definition there exists U' such that $U \mathrel{\dot{\approx}^\bullet} U'$ and $!U' \mathrel{\dot{\approx}^\circ} Q$. We have three cases to consider for A:

- A is a process T: therefore we have $U \xrightarrow{l} T$. By induction, there exists T' such that $U' \stackrel{l}{\Rightarrow} T'$ and $T\ (\dot{\approx})^\bullet_c\ T'$. By LTS-REPLIC and several applications of LTS-PAR, we have $!U' \stackrel{l}{\Rightarrow} T' \mid !U'$, and since $!U' \mathrel{\dot{\approx}^\circ} Q$, there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and $T' \mid !U' \mathrel{\dot{\approx}^\circ} Q'$. Using CONG twice, we have $T \mid !U \mathrel{\dot{\approx}^\bullet} T' \mid !U'$, so by OPEN RIGHT we have $a[T]\ (\dot{\approx})^\bullet_c\ Q'$ as required.

- A is an abstraction F: therefore we have $U \xrightarrow{a} F$. Let $T\ (\dot{\approx})^\bullet_c\ T'$ be closed processes. By induction, there exists G, U'' such that $U' \stackrel{b}{\Rightarrow} G$, $G \circ T' \stackrel{\tau}{\Rightarrow} U''$, and $F \circ T\ (\dot{\approx})^\bullet_c\ U''$. By CONG used twice, we have $(F \mid !U) \circ T\ (\dot{\approx})^\bullet_c\ U'' \mid !U'$.

  By LTS-REPLIC and several application of rule LTS-PAR, we have $!U' \stackrel{a}{\Rightarrow} G \mid !U'$, and since $!U' \mathrel{\dot{\approx}^\circ} Q$, there exists F', Q'' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ T' \stackrel{\tau}{\Rightarrow} Q''$, and $(G \mid !U') \circ T' \mathrel{\dot{\approx}^\circ} Q''$. We have $G \circ T' \stackrel{\tau}{\Rightarrow} U''$, so by LTS-PAR we have $(G \mid !U') \circ T' \stackrel{\tau}{\Rightarrow} U'' \mid !U'$. Hence there exists Q' such that $Q'' \stackrel{\tau}{\Rightarrow} Q'$ and $U'' \mid !U' \mathrel{\dot{\approx}^\circ} Q'$. We then have $F \circ T\ (\dot{\approx})^\bullet_c\ Q'$ by OPEN RIGHT.

- A is a concretion $\langle R\rangle S$: therefore we have $U \xrightarrow{\overline{a}} \langle R\rangle S$. By induction, there exists $\langle R''\rangle U''$, S'' such that $U' \stackrel{\overline{a}}{\Rightarrow} \langle R''\rangle U''$, $U'' \stackrel{\tau}{\Rightarrow} S''$, $R\ (\dot{\approx})^\bullet_c\ R''$, and $S\ (\dot{\approx})^\bullet_c\ S''$. By CONG used twice, we have $S \mid !U\ (\dot{\approx})^\bullet_c\ S' \mid !U'$.

  By LTS-REPLIC and several application of rule LTS-PAR, we have $!U' \stackrel{\overline{a}}{\Rightarrow} \langle R''\rangle U'' \mid !U'$, and since we have $!U' \mathrel{\dot{\approx}^\circ} Q$, there exists $\langle R'\rangle Q''$, Q' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R'\rangle Q''$, $Q'' \stackrel{\tau}{\Rightarrow} Q'$, $R'' \mathrel{\dot{\approx}^\circ} R'$, and $U'' \mid !U' \mathrel{\dot{\approx}^\circ} Q'$. We have $U'' \stackrel{\tau}{\Rightarrow} S''$, so by LTS-PAR we have $U'' \mid !U' \stackrel{\tau}{\Rightarrow} S'' \mid !U'$. Hence there exists S' such that $Q' \stackrel{\tau}{\Rightarrow} S'$ and $S'' \mid !U' \mathrel{\dot{\approx}^\circ} S'$. Finally we have $R\ (\dot{\approx})^\bullet_c\ R'$ and $S \mid !U\ (\dot{\approx})^\bullet_c\ S'$ by OPEN RIGHT.

□

As a corollary, we have

Lemma 31. *If $P\ (\dot{\approx})^\bullet_c\ Q$ then:*

- *If $P \stackrel{l}{\Rightarrow} P'$, then there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and $P'\ (\dot{\approx})^\bullet_c\ Q'$.*

- *If $P \overset{a}{\Rightarrow} F$, for all R, there exists F', Q' such that $Q \overset{a}{\Rightarrow} F'$, $F' \circ R \overset{\tau}{\Rightarrow} Q'$ and $F \circ R\ (\dot{\approx})^\bullet_c\ Q'$*

- *If $P \overset{\overline{a}}{\Rightarrow} \langle R \rangle S$, there exists R', S', S'' such that $Q \overset{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \overset{\tau}{\Rightarrow} S'$, $R\ (\dot{\approx})^\bullet_c\ R'$, and $S\ (\dot{\approx})^\bullet_c\ S'$.*

Proof. By induction on $P \overset{\alpha}{\Rightarrow} A$. In the abstraction case, we also use the reflexivity of $(\dot{\approx})^\bullet_c$ (we have $R\ (\dot{\approx})^\bullet_c\ R$ for all closed process R). $\square$

With this result we can show the following lemma:

Lemma 32. *The transitive and reflexive closure of $(\dot{\approx})^\bullet_c$ is an early weak bisimulation.*

Proof. With property SYMM it is enough to show that $((\dot{\approx})^\bullet_c)^*$ is a simulation. Let P, Q such that $P((\dot{\approx})^\bullet_c)^* Q$. There exists $k \geq 0$ such that $P((\dot{\approx})^\bullet_c)^k Q$. The proof is by induction on k. There is nothing to show for $k = 0$ since $((\dot{\approx})^\bullet_c)^*$ is reflexive.

We suppose the result holds up to k. We have $P\ (\dot{\approx})^\bullet_c\ P_1 \dots P_{k-1}\ (\dot{\approx})^\bullet_c\ Q$ and $P \xrightarrow{a} A$. We have three cases to consider.

- A is a process P'. By induction there exists P'_{k-1} such that $P_{k-1} \overset{l}{\Rightarrow} P'_{k-1}$ and $P'((\dot{\approx})^\bullet_c)^* P'_{k-1}$. By lemma 31, there exists Q' such that $Q \overset{l}{\Rightarrow} Q'$ and $P'_{k-1}\ (\dot{\approx})^\bullet_c\ Q'$. We have $P'((\dot{\approx})^\bullet_c)^* Q'$ by transitivity.

- A is an abstraction F. Let R be a closed process. By induction there exists F_{k-1}, P'_{k-1} such that $P_{k-1} \overset{a}{\Rightarrow} F_{k-1}$, $F_{k-1} \circ R \overset{\tau}{\Rightarrow} P'_{k-1}$ and $F \circ R((\dot{\approx})^\bullet_c)^* P'_{k-1}$. By lemma 31, there exists F', Q'' such that $Q \overset{a}{\Rightarrow} F'$, $F' \circ R \overset{\tau}{\Rightarrow} Q''$ and $F_{k-1} \circ R\ (\dot{\approx})^\bullet_c\ Q''$. Since $F_{k-1} \circ R \overset{\tau}{\Rightarrow} P'_{k-1}$, there exists Q' such that $Q'' \overset{\tau}{\Rightarrow} Q'$ and $P'_{k-1}\ (\dot{\approx})^\bullet_c\ Q'$. We have $F \circ R((\dot{\approx})^\bullet_c)^* Q'$ by transitivity.

- A is a concretion $\langle R \rangle S$. By induction there exists $R_{k-1}, S_{k-1}, S'_{k-1}$ such that $P_{k-1} \overset{\overline{a}}{\Rightarrow} \langle R_{k-1} \rangle S'_{k-1}$, $S'_{k-1} \overset{\tau}{\Rightarrow} S_{k-1}$, $R((\dot{\approx})^\bullet_c)^* R_{k-1}$, and $S((\dot{\approx})^\bullet_c)^* S_{k-1}$. By lemma 31, there exists $\langle R' \rangle Q''$, Q' such that $Q \overset{\overline{a}}{\Rightarrow} \langle R' \rangle Q''$, $Q'' \overset{\tau}{\Rightarrow} Q'$, $R_{k-1}\ (\dot{\approx})^\bullet_c\ R'$, and $S'_{k-1}\ (\dot{\approx})^\bullet_c\ Q'$. Since $S'_{k-1} \overset{\tau}{\Rightarrow} S_{k-1}$, there exists S' such that $Q' \overset{\tau}{\Rightarrow} S'$ and $S_{k-1}\ (\dot{\approx})^\bullet_c\ S'$. We have $R((\dot{\approx})^\bullet_c)^* R'$ and $S((\dot{\approx})^\bullet_c)^* S'$ by transitivity.

$\square$

To prove that $\dot{\approx}$ is a congruence, it is enough to prove the following lemma:

Lemma 33. $\dot{\approx}^\bullet = \dot{\approx}^\circ$

Proof. By lemma 32 we have $(\dot{\approx})^{\bullet *}_c \subseteq \dot{\approx}$, so we have $(\dot{\approx})^{\bullet * \circ}_c \subseteq \dot{\approx}^\circ$. We now prove that $\dot{\approx}^\bullet \subseteq (\dot{\approx})^{\bullet \circ}_c$. Let P, Q such that $P \dot{\approx}^\bullet Q$. For all σ which closes P, Q, we have $P\sigma \dot{\approx}^\bullet Q\sigma$ by SUBST. Since the considered processes are closed, we have $P\sigma\ (\dot{\approx})^{\bullet}_{c}\ Q\sigma$. Consequently, we have $P\ (\dot{\approx})^{\bullet\circ}_{c}\ Q$. Hence we have $\dot{\approx}^{\bullet} \subseteq (\dot{\approx})^{\bullet\circ}_{c} \subseteq (\dot{\approx})^{\bullet\circ *}_{c} \subseteq \dot{\approx}^{\circ}$, i.e. $\dot{\approx}^{\bullet} \subseteq \dot{\approx}^{\circ}$. The reverse inclusion is given by Open, so we have $\dot{\approx}^{\bullet} = \dot{\approx}^{\circ}$.

□

E Completeness proofs for HOP

E.1 Strong case

Lemma 34. *For all actions α, the relation $\xrightarrow{\alpha}$ is image-finite.*

Proof. By induction on the shape of P, as in HOπP. We just add the case $P = Q + R$. By LTS-Sum, the possible reductions from P are the one from Q and the one from R, which are finite by induction hypothesis.

□

Definition 34. *The relation $\dot{\sim}_\omega$ is defined on closed processes by:*

1. *We have $P \dot{\sim}_0 Q$ for all processes P, Q.*
2. *$P \dot{\sim}_{k+1} Q$ iff*
   - *If $P \xrightarrow{l} P'$, then there exists Q' such that $Q \xrightarrow{l} Q'$ and $P' \dot{\sim}_k Q'$, and conversely if $Q \xrightarrow{l} Q'$.*
   - *If $P \xrightarrow{a} F$, then for all closed processes R, there exists F' such that $Q \xrightarrow{a} F'$ and $F' \circ R \dot{\sim}_k F \circ R$, and conversely if $Q \xrightarrow{a} F$.*
   - *If $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S' such that $Q \xrightarrow{\overline{a}} \langle R' \rangle S'$ and $R \dot{\sim}_k R', S \dot{\sim}_k S'$, and conversely if $Q \xrightarrow{\overline{a}} C$.*
3. *$\dot{\sim}_\omega = \bigcap_k \dot{\sim}_k$*

Lemma 35. *The relations $\dot{\sim}$ and $\dot{\sim}_\omega$ coincide.*

The proof is similar to the HOπP one. In the following, we write $\tau.P + s$ for $(\tau.P) + s.\mathbf{0}$.

Lemma 36. *Let P, Q two closed processes. For all integers k, if $P \not\dot{\sim}_k Q$ then there exists a context $\mathbb{K}$ such that $\mathbb{K}\{P\} \not\approx_b \mathbb{K}\{Q\}$.*

Proof. We proceed by induction on k. There is nothing to prove for $n = 0$.

Assume the property holds for all $k \leq n$. We now prove it for $n + 1$. We distinguish the following cases :

- $P \xrightarrow{\tau} P'$. For all Q' such that $Q \xrightarrow{\tau} Q'$, we have $P' \not\dot{\sim}_k Q'$. Since $\xrightarrow{\tau}$ is image-finite, the set $\{Q'_i | Q \xrightarrow{\tau} Q'_i\}$ is finite. By induction, there are contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{P'\} \not\approx_b \mathbb{K}_i\{Q'_i\}$ for all i. We define:

$$\mathbb{K} = a[\square] \mid a(X) \sum_i \tau.(\tau.\mathbb{K}_i\{X\} + d_i)$$

where $(d_i)_i, a$ do not occur in P, Q. Assume that $\mathbb{K}\{P\} \sim_b \mathbb{K}\{Q\}$. Since $P \longrightarrow P'$, we have

$$\mathbb{K}\{P\} \longrightarrow a[P'] \mid a(X) \sum_j \tau.(\tau.\mathbb{K}_j\{X\} + d_j) = R_1$$

This reduction can only be matched by

$$\mathbb{K}\{Q\} \longrightarrow a[Q'_i] \mid a(X) \sum_j \tau.(\tau.\mathbb{K}_j\{X\} + d_j) = S_1$$

for some i. We now have

$$R_1 \longrightarrow \sum_j \tau.(\tau.\mathbb{K}_j\{P'\} + d_j) = R_2$$

which can only be matched by

$$S_1 \longrightarrow \sum_j \tau.(\tau.\mathbb{K}_j\{Q'_i\} + d_j) = S_2$$

since $\neg R_2 \downarrow_a$. We have $R_2 \longrightarrow \tau.\mathbb{K}_i\{P'\} + d_i = R_3$, which can only be matched by $S_3 \longrightarrow \tau.\mathbb{K}_i\{Q'_i\} + d_i = S_3$, since $R_3 \downarrow_{d_i}$. Finally we have $R_3 \longrightarrow \mathbb{K}_i\{P'\}$, which is matched by $S_3 \longrightarrow \mathbb{K}_i\{Q'_i\}$. Hence a contradiction, since $\mathbb{K}_i\{P'\} \not\sim_b \mathbb{K}_i\{Q'_i\}$, so we have $\mathbb{K}\{P\} \not\sim_b \mathbb{K}\{Q\}$ as required.

- $P \xrightarrow{m} P'$ For all Q' such that $Q \xrightarrow{m} Q'$, we have $P' \not\simeq_k Q'$. Since $\xrightarrow{l}$ is image-finite, the set $\{Q'_i | Q \xrightarrow{m} Q'_i\}$ is finite. By induction, there are contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{P'\} \not\sim_b \mathbb{K}_i\{Q'_i\}$ for all i. We define :

$$\mathbb{K} = a[\Box] \mid \overline{m}.a(X) \sum_i \tau.(\tau.\mathbb{K}_i\{X\} + d_i)$$

where $(d_i)_i, a$ do not occur in P, Q. Assume that $\mathbb{K}\{P\} \sim_b \mathbb{K}\{Q\}$. We have

$$\mathbb{K}\{P\} \longrightarrow a[P'] \mid a(X) \sum_j \tau.(\tau.\mathbb{K}_j\{X\} + d_j) = R_1$$

Since $R_1 \downarrow_a$, it can only be matched by

$$\mathbb{K}\{Q\} \longrightarrow a[Q'_i] \mid a(X) \sum_j \tau.(\tau.\mathbb{K}_j\{X\} + d_j) = S_1$$

From here, the proof is similar to the previous case.

- $P \xrightarrow{\overline{m}} P'$ Similar to the case above, with m instead of $\overline{m}$ in $\mathbb{K}$.

- $P \xrightarrow{a} F = (X)V$. There exists a process T such that for all F' such that $Q \xrightarrow{a} F'$, we have $F \circ T \not\approx_k F' \circ T$. Since $\xrightarrow{a}$ is image-finite, the set $\{F'_i | Q \xrightarrow{a} F'_i\}$ is finite. By induction, there are contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{F'_i \circ T\} \not\approx_b \mathbb{K}_i\{F \circ T\}$. We define:

$$\mathbb{K} = b[\Box] \mid \overline{a}\langle T\rangle b(X) \sum_i \tau.(\tau.\mathbb{K}_i\{X\} + d_i)$$

where $b, (d_i)$ are all distinct, and do not occur in T, P, Q. We have

$$\mathbb{K}\{P\} \longrightarrow b[F \circ T] \mid b(X) \sum_j \tau.(\tau.\mathbb{K}_j\{X\} + d_j) = R_1$$

Since $R_1 \downarrow_b$, it can only be matched by a

$$\mathbb{K}\{Q\} \longrightarrow b[F'_i \circ T] \mid b(X) \sum_j \tau.(\tau.\mathbb{K}_j\{X\} + d_j) = S_1$$

for some i. Now we have

$$R_1 \longrightarrow \sum_j \tau.(\tau.\mathbb{K}_j\{F \circ T\} + d_j) = R_2$$

Since $\neg R_2 \downarrow_b$, it is matched by :

$$S_1 \longrightarrow \sum_j \tau.(\tau.\mathbb{K}_j\{F'_i \circ T\} + d_j) = S_2$$

In turn, we have

$$R_2 \longrightarrow \tau.\mathbb{K}_i\{F \circ T\} + d_i = R_3$$

Since $R_3 \downarrow_{d_i}$, it can only be matched by the reduction

$$S_2 \longrightarrow \tau.\mathbb{K}_i\{F'_i \circ T\} + d_i = S_3$$

Finally we have $R_3 \longrightarrow \mathbb{K}_i\{F \circ T\}$, which is matched by $S_3 \longrightarrow \mathbb{K}_i\{F'_i \circ T\}$. Hence a contradiction since by assumption we have $\mathbb{K}_i\{F \circ T\} \not\approx_b \mathbb{K}_i\{F'_i \circ T\}$. So we have $\mathbb{K}\{P\} \not\approx_b \mathbb{K}\{Q\}$ as required.

- $P \xrightarrow{\overline{a}} \langle R\rangle S$. For all $\langle R'\rangle S'$ such that $Q \xrightarrow{\overline{a}} \langle R'\rangle S'$, we have $R \not\approx_k R'$ or $S \not\approx_k S'$. Since $\xrightarrow{\overline{a}}$ is image-finite, the set $\{C_i | Q \xrightarrow{\overline{a}} C_i\}$ is finite. By induction, there exists contexts $\mathbb{K}_i$ such that $\mathbb{K}_i\{R\} \not\approx_b \mathbb{K}_i\{R_i\}$ or $\mathbb{K}_i\{S\} \not\approx_b \mathbb{K}_i\{S_i\}$ for all i. We define then :

$$\mathbb{K} = b[\Box] \mid a(X)b(Y) \sum_i \tau.(\tau.(\tau.\mathbb{K}_i\{X\} + e) + \tau.(\tau.\mathbb{K}_i\{Y\} + f) + d_i)$$

where $b, (d_i), e, f$ are all distinct and do not occur in P, Q. We have:

$$\mathbb{K}\{P\} \longrightarrow b[S] \mid b(Y) \sum_j \tau.(\tau.(\tau.\mathbb{K}_j\{R\} + e) + \tau.(\tau.\mathbb{K}_j\{Y\} + f) + d_j) = P_2$$

Since $P_2 \downarrow_b$, it is matched by

$$\mathbb{K}\{Q\} \longrightarrow b[S_i] \mid b(Y) \sum_j \tau.(\tau.(\tau.\mathbb{K}_j\{R_i\} + e) + \tau.(\tau.\mathbb{K}_j\{Y\} + f) + d_j) = Q_2$$

for some i. Now we have

$$P_2 \longrightarrow \sum_j \tau.(\tau.(\tau.\mathbb{K}_j\{R\} + e) + \tau.(\tau.\mathbb{K}_j\{S\} + f) + d_j) = P_3$$

which is matched by:

$$Q_2 \longrightarrow \sum_j \tau.(\tau.(\tau.\mathbb{K}_j\{R_i\} + e) + \tau.(\tau.\mathbb{K}_j\{S_i\} + f) + d_j) = Q_3$$

since $\neg P_3 \downarrow_b$. We have now:

$$P_3 \longrightarrow \tau.(\tau.\mathbb{K}_i\{R\} + e) + \tau.(\tau.\mathbb{K}_i\{S\} + f) + d_i = P_4$$

Since $P_4 \downarrow_{d_i}$, it is matched by:

$$Q_3 \longrightarrow \tau.(\tau.\mathbb{K}_i\{R_i\} + e) + \tau.(\tau.\mathbb{K}_i\{S_i\} + f) + d_i = Q_4$$

We suppose that for this particular i we have $\mathbb{K}_i\{R\} \not\approx_b \mathbb{K}_i\{R_i\}$. We have:

$$P_4 \longrightarrow \tau.\mathbb{K}_i\{R\} + e = P_5$$

since $P_5 \downarrow_e$, it is matched by:

$$Q_4 \longrightarrow \tau.\mathbb{K}_i\{R_i\} + e = Q_5$$

We have $P_5 \longrightarrow \mathbb{K}_i\{R\}$, which is matched by $Q_5 \longrightarrow \mathbb{K}_i\{R_i\}$. We have $\mathbb{K}_i\{R\} \not\approx_b \mathbb{K}_i\{R_i\}$, hence a contradiction.

We suppose now that $\mathbb{K}_i\{S\} \not\approx_b \mathbb{K}_i\{S_i\}$. We have:

$$P_4 \longrightarrow \tau.\mathbb{K}_i\{S\} + f = P_5$$

since $P_5 \downarrow_f$, it is matched by:

$$Q_4 \longrightarrow \tau.\mathbb{K}_i\{S_i\} + f = Q_5$$

We have $P_5 \longrightarrow \mathbb{K}_i\{S\}$, which is matched by $Q_5 \longrightarrow \mathbb{K}_i\{S_i\}$. We have $\mathbb{K}_i\{S\} \not\approx_b \mathbb{K}_i\{S_i\}$, hence a contradiction.

$\square$

E.2 Weak case

Definition 35. *The relation $\dot{\approx}_\omega$ is defined on closed processes by:*

1. *We have $P \dot{\approx}_0 Q$ for all processes P, Q.*
2. *$P \dot{\approx}_{k+1} Q$ iff*
   - *If $P \xrightarrow{l} P'$, then there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and $P' \dot{\approx}_k Q'$, and conversely if $Q \xrightarrow{l} Q'$.*
   - *If $P \xrightarrow{a} F$, then for all closed processes R, there exists F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ R \stackrel{\tau}{\Rightarrow} Q'$ and $Q' \dot{\approx}_k F \circ R$, and conversely if $Q \xrightarrow{a} F$.*
   - *If $P \xrightarrow{\overline{a}} \langle R \rangle S$, there exists R', S', S'' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R' \rangle S''$, $S'' \stackrel{\tau}{\Rightarrow} S'$, $R \dot{\approx}_k R'$, $S \dot{\approx}_k S'$, and conversely if $Q \xrightarrow{\overline{a}} C$.*
3. *$\dot{\approx}_\omega = \bigcap_k \dot{\approx}_k$*

Lemma 37. *The relation $\dot{\approx}$ and $\dot{\approx}_\omega$ coincide on image-finite processes.*

Proof. From the definition of $\dot{\approx}_\omega$, we already have that $\dot{\approx} \subset \dot{\approx}_\omega$. We show the converse by proving that $\dot{\approx}_\omega$ is a weak bisimulation. Let P, Q be image-finite processes such that $P \dot{\approx}_\omega Q$. Since the relation is symmetrical, we make the proof for the transitions from P only. We have three cases to check:

- Assume $P \xrightarrow{l} P'$. For all integers k, there exists Q_k such that $Q \stackrel{l}{\Rightarrow} Q_k$ and $P' \dot{\approx}_k Q_k$. Since Q is image-finite, the set $\{Q_i | Q \stackrel{l}{\Rightarrow} Q_i\}$ is finite. We now prove by contradiction that there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and for all k, $P' \dot{\approx}_k Q'$. Assume that for all Q_i such that $Q \stackrel{l}{\Rightarrow} Q_i$, there exists k_i such that $P' \dot{\not\approx}_{k_i} Q_i$. Since $\dot{\approx}_m \subset \dot{\approx}_l$ if $l \leq m$, for all $m \geq k_i$, we have $P' \dot{\not\approx}_m Q_i$. Since $\{Q_i | Q \stackrel{l}{\Rightarrow} Q_i\}$ is finite, the set $\{k_i\}$ is finite and has a greatest element M. For all Q' such that $Q \stackrel{l}{\Rightarrow} Q'$, we have $P' \dot{\not\approx}_m Q'$ for all $m \geq M$. But for all k, there exists Q_k such that $Q \stackrel{l}{\Rightarrow} Q_k$ and $P' \dot{\approx}_k Q_k$, hence a contradiction. Therefore there exists Q' such that $Q \stackrel{l}{\Rightarrow} Q'$ and for all k, $P' \dot{\approx}_k Q'$, i.e. $P' \dot{\approx}_\omega Q'$ as required.
- Assume $P \xrightarrow{a} F$. Let R be a closed process. For all k, there exists F_k, Q_k such that $Q \stackrel{a}{\Rightarrow} F_k$, $F_k \circ R \stackrel{\tau}{\Rightarrow} Q_k$ and $F \circ R \dot{\approx}_k Q_k$. Since Q is image-finite, the sets $\{F_i | Q \stackrel{a}{\Rightarrow} F_i\}$ and $\{Q_i | \exists F_i, Q \stackrel{a}{\Rightarrow} F_i \text{ and } F_i \circ R \stackrel{\tau}{\Rightarrow} Q_i\}$ are finite. By contradiction we can show that there exists F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \circ R \stackrel{\tau}{\Rightarrow} Q'$ and for all k, $Q' \dot{\approx}_k F \circ R$, i.e. $Q' \dot{\approx}_\omega F \circ R$ as required.
- Assume $P \xrightarrow{\overline{a}} C = \langle R \rangle S$. For all k, there exists $C_k = \langle R_k \rangle S'_k$, S_k such that $Q \stackrel{\overline{a}}{\Rightarrow} C_k$, $S'_k \stackrel{\tau}{\Rightarrow} S_k$, $R \dot{\approx}_k R_k$ and $S \dot{\approx}_k S_k$. Since Q is image-finite, the sets $\{C_i | Q \stackrel{\overline{a}}{\Rightarrow} C_i\}$ and $\{S_i | \exists \langle R_i \rangle S'_i, Q \stackrel{a}{\Rightarrow} \langle R_i \rangle S'_i \text{ and } S'_i \stackrel{\tau}{\Rightarrow} S_i\}$ are finite.

By contradiction we can show that there exists $C' = \langle R' \rangle S''$, S' such that $Q \stackrel{\overline{a}}{\Rightarrow} C'$, $S'' \stackrel{\tau}{\Rightarrow} S'$ and for all k, $R \dot{\approx}_k R'$, $S \dot{\approx}_k S'$, i.e. $R \dot{\approx}_\omega R'$, $S \dot{\approx}_\omega S'$ as required.

$\square$

Lemma 38. *Let P, Q two closed image-finite processes. For all integers k, if $P \dot{\not\approx}_k Q$ then there exists a context $\mathbb{K}$ and a name d such that $\mathbb{K}\{P\} + d \not\approx_b \mathbb{K}\{Q\} + d$.*

Proof. We proceed by induction on k. There is nothing to prove for $n = 0$.

Assume the property holds for all $k \leq n$. We now prove it for $n + 1$. We distinguish the following cases :

- $P \xrightarrow{\tau} P'$. For all Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$, we have $P' \dot{\not\approx}_k Q'$. Since Q is image-finite, the set $\{Q'_i | Q \stackrel{\tau}{\Rightarrow} Q'_i\}$ is finite. By induction, there are contexts $\mathbb{K}_i$ and names d_i such that $\mathbb{K}_i\{P'\} + d_i \not\approx_b \mathbb{K}_i\{Q'_i\} + d_i$ for all i. We define:

$$\mathbb{K} = a[\square] \mid a(X)(s + \sum_i \tau.(\mathbb{K}_i\{X\} + d_i))$$

where a, s do not occur in P, Q. Let t be a fresh name. Assume that $\mathbb{K}\{P\} + t \approx_b \mathbb{K}\{Q\} + t$. Since $P \longrightarrow P'$, we have

$$\mathbb{K}\{P\} + t \longrightarrow a[P'] \mid a(X)(s + \sum_j \tau.(\mathbb{K}_j\{X\} + d_j)) = R_1$$

Since $\neg R_1 \downarrow_t$ and $\neg R_1 \downarrow_a$ (the passivation of locality a is not triggered), it can only be matched by

$$\mathbb{K}\{Q\} + t \Longrightarrow a[Q'_l] \mid a(X)(s + \sum_j \tau.(\mathbb{K}_j\{X\} + d_j)) = S_1$$

for some l. We now have

$$R_1 \longrightarrow s + \sum_j \tau.(\mathbb{K}_j\{P'\} + d_j) = R_2$$

Since we have $\neg R_2 \downarrow_a$ and $R_2 \downarrow_s$, it can only be matched by:

$$S_1 \Longrightarrow s + \sum_j \tau.(\mathbb{K}_j\{Q'_i\} + d_j) = S_2$$

with $Q'_l \Longrightarrow Q'_i$ for some i. We have $R_2 \longrightarrow \mathbb{K}_i\{P'\} + d_i = R_3$, which can only be matched by $S_2 \Longrightarrow \mathbb{K}_i\{Q'_i\} + d_i = S_3$, since $R_3 \downarrow_{d_i}$. Hence a contradiction, since $\mathbb{K}_i\{P'\} + d_i \not\approx_b \mathbb{K}_i\{Q'_i\} + d_i$, so we have $\mathbb{K}\{P\} + t \not\approx_b \mathbb{K}\{Q\} + t$ as required.

- $P \xrightarrow{m} P'$ For all Q' such that $Q \stackrel{m}{\Rightarrow} Q'$, we have $P' \not\approx_k Q'$. Since Q is image-finite, the set $\{Q'_i | Q \stackrel{m}{\Rightarrow} Q'_i\}$ is finite. By induction, there are contexts $\mathbb{K}_i$ and names d_i such that $\mathbb{K}_i\{P'\} + d_i \not\approx_b \mathbb{K}_i\{Q'_i\} + d_i$ for all i. We define :

$$\mathbb{K} = a[\Box] \mid \overline{m}.a(X)(s + \sum_i \tau.(\mathbb{K}_i\{X\} + d_i))$$

where s, a do not occur in P, Q. Let t be a fresh name. Assume that $\mathbb{K}\{P\} + t \approx_b \mathbb{K}\{Q\} + t$. We have

$$\mathbb{K}\{P\} + t \longrightarrow a[P'] \mid a(X)(s + \sum_j \tau.(\mathbb{K}_j\{X\} + d_j)) = R_1$$

Since $R_1 \downarrow_a$, it can only be matched by

$$\mathbb{K}\{Q\} + t \Longrightarrow a[Q'_l] \mid a(X)(s + \sum_j \tau.(\mathbb{K}_j\{X\} + d_j)) = S_1$$

From here, the proof is similar to the previous case.

- $P \xrightarrow{\overline{m}} P'$ Similar to the case above, with m instead of $\overline{m}$ in $\mathbb{K}$.

- $P \xrightarrow{a} F = (X)V$. There exists a process T such that for all F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$ and $F' \circ T \stackrel{\tau}{\Rightarrow} Q'$, we have $F \circ T \not\approx_k Q'$. Since Q is image-finite, the sets $\{F'_i | Q \stackrel{a}{\Rightarrow} F'_i\}$ and $\{Q'_i | \exists F_i, Q \stackrel{a}{\Rightarrow} F_i \text{ and } F_i \circ T \stackrel{\tau}{\Rightarrow} Q'_i\}$ are finite. By induction, there are contexts $\mathbb{K}_i$ and names (d_i) such that $\mathbb{K}_i\{Q'_i\} + d_i \not\approx_b \mathbb{K}_i\{F \circ T\} + d_i$. We define:

$$\mathbb{K} = b[\Box] \mid \overline{a}\langle T\rangle b(X)(s + \sum_i \tau.(\mathbb{K}_i\{X\} + d_i))$$

where b, s are distinct, and do not occur in T, P, Q. Let t be a fresh name. We have

$$\mathbb{K}\{P\} + t \longrightarrow b[F \circ T] \mid b(X)(s + \sum_j \tau.(\mathbb{K}_j\{X\} + d_j)) = R_1$$

Since $R_1 \downarrow_b$, it can only be matched by a

$$\mathbb{K}\{Q\} + t \Longrightarrow b[Q'_l] \mid b(X)(s + \sum_j \tau.(\mathbb{K}_j\{X\} + d_j)) = S_1$$

for some l. From here, the proof is similar to the $P \xrightarrow{\tau} P'$ case.

- $P \xrightarrow{\overline{a}} \langle R\rangle S$. For all $\langle R'\rangle S''$, S' such that $Q \stackrel{\overline{a}}{\Rightarrow} \langle R'\rangle S''$ and $S'' \stackrel{\tau}{\Rightarrow} S'$, we have $R \not\approx_k R'$ or $S \not\approx_k S'$. Since Q is image-finite, the sets $\{C_i | Q \stackrel{\overline{a}}{\Rightarrow} C_i\}$ and $\{S_{i,j} | \exists \langle R'_i\rangle S'_i, Q \stackrel{a}{\Rightarrow} \langle R'_i\rangle S'_i \text{ and } S'_i \stackrel{\tau}{\Rightarrow} S_{i,j}\}$ are finite. By induction, for $i \in I$ such that $R \not\approx_b R_i$, there exists contexts $\mathbb{K}_i$ and names d_i such that $\mathbb{K}_i\{R\} + d_i \not\approx_b \mathbb{K}_i\{R_i\} + d_i$. Otherwise, for $i \in J$ such that $R \approx_b R_i$, there exists contexts $\mathbb{K}_{i,j}$ and names $d_{i,j}$ such that $\mathbb{K}_{i,j}\{S\} + d_{i,j} \not\approx_b \mathbb{K}_{i,j}\{S_{i,j}\} + d_{i,j}$ for all j. We define:

$$\mathbb{K} = b[\Box] \mid a(X)b(Y)(s + \sum_{i \in I} \tau.(\mathbb{K}_i\{X\} + d_i) + \sum_{i \in J} \sum_j \tau.(\mathbb{K}_{i,j}\{Y\} + d_{i,j}))$$

where b, s are distinct and do not occur in P, Q. Let t be a fresh name. We have:

$$\mathbb{K}\{P\} + t \longrightarrow b[S] \mid b(Y)(s + \sum_{i \in I} \tau.(\mathbb{K}_i\{R\} + d_i) + K') = P_2$$

with $K' = \sum_{i \in J} \sum_j \tau.(\mathbb{K}_{i,j}\{Y\} + d_{i,j})$. Since $P_2 \downarrow_b$, it is matched by

$$\mathbb{K}\{Q\} + t \Longrightarrow b[S_{l,m}] \mid b(Y)(s + \sum_{i \in I} \tau.(\mathbb{K}_i\{R_l\} + d_i) + K') = Q_2$$

for some l, m. Now we have:

$$P_2 \longrightarrow s + \sum_{i \in I} \tau.(\mathbb{K}_i\{R\} + d_i) + \sum_{i \in J} \sum_j \tau.(\mathbb{K}_{i,j}\{S\} + d_{i,j}) = P_3$$

Since $P_3 \downarrow_s$, it is matched by:

$$Q_2 \Longrightarrow s + \sum_{i \in I} \tau.(\mathbb{K}_i\{R_l\} + d_i) + \sum_{i \in J} \sum_j \tau.(\mathbb{K}_{i,j}\{S_{l,n}\} + d_{i,j}) = Q_3$$

for some n such that $S_{l,m} \Longrightarrow S_{l,n}$. We suppose that $l \in I$, i.e. we have $R \not\approx_b R_l$. We have

$$P_3 \longrightarrow \mathbb{K}_l\{R\} + d_l = P_4$$

which is matched by:

$$Q_3 \Longrightarrow \mathbb{K}_l\{R_l\} + d_l = Q_4$$

since $P_4 \downarrow_{d_l}$. We have $P_4 \not\approx_b Q_4$ by induction hypothesis, hence we have $\mathbb{K}\{P\} + t \not\approx_b \mathbb{K}\{Q\} + t$ as required.

We suppose now that $l \in J$, i.e. we have $R \approx_b R_l$. We have

$$P_3 \longrightarrow \mathbb{K}_{l,n}\{S\} + d_{l,n} = P_4$$

which is matched by:

$$Q_3 \Longrightarrow \mathbb{K}_{l,n}\{S_{l,n}\} + d_{l,n} = Q_4$$

since $P_4 \downarrow_{d_{l,n}}$. We have $P_4 \not\approx_b Q_4$ by induction hypothesis, hence we have $\mathbb{K}\{P\} + t \not\approx_b \mathbb{K}\{Q\} + t$ as required.

$\Box$

F Normal bisimulation

F.1 Strong case

Lemma 39. *Let $\mathbb{E}$ be an evolution context and $P \xrightarrow{\alpha} A$. Then $\mathbb{E}\{P\} \xrightarrow{\alpha} \mathbb{E}'\{A\}$ and the hole in $\mathbb{E}'$ is not under a replication or choice operator.*

Proof. Immediate by induction on $\mathbb{E}$, and considering the rules LTS-Par, LTS-Loc, LTS-Replic, LTS-Sum.

□

Lemma 40. *Let P, Q such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. Suppose we have $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/Y\} = P_n$ matched by $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/Y\} = Q_n$ with $P_n \dot{\sim}_l Q_n$. One of the following holds:*

- *There exists P_1, Q_1 such that $P_n = n.\mathbf{0} \mid P_1$, $Q_n = n.\mathbf{0} \mid Q_1$ with $P_1 \dot{\sim}_l Q_1$.*
- *There exists $a_1, \dots a_k$, $P_1 \dots P_{k+1}$, $Q_1 \dots Q_{k+1}$ such that*

$$P_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$$

  and

$$Q_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$$

  and for all $1 \leq j \leq k+1$, $P_j \dot{\sim}_l Q_j$.

Proof. Since P_n can only perform one $\xrightarrow{n}$ transition, we can detect if $n.\mathbf{0}$ is in a locality or not: if there exists a transition $P_n \xrightarrow{\overline{a}} \langle R'n \rangle S'_n$ for some a such that R'_n may perform a transition $\xrightarrow{n}$, then the transition is a passivation and the process $n.\mathbf{0}$ is in a locality in P_n. Otherwise, $n.\mathbf{0}$ is not in a locality.

By lemma 39, $n.\mathbf{0}$ is only under localities and parallel compositions in P_n and Q_n.

We show that if $n.\mathbf{0}$ is not under a locality in P_n, it is also not under a locality in Q_n. Suppose $n.\mathbf{0}$ is not in a locality in P_n and is in a locality in Q_n. We have $Q_n \xrightarrow{\overline{a}} \langle \mathbb{E}\{n.\mathbf{0}\} \rangle Q''$ for some $a, \mathbb{E}, Q''$. These transitions can only be matched by a passivation of $n.\mathbf{0}$ in P_n, which is impossible by hypothesis, hence a contradiction. We have the same reasoning if $n.\mathbf{0}$ is in a locality in P_n and not in a locality in Q_n. Therefore if $n.\mathbf{0}$ is not in a locality in P_n, it is not in a locality in Q_n. Consequently in this case, there exists P_1, Q_1 such that $P_n = n.\mathbf{0} \mid P_1$ and $Q_n = n.\mathbf{0} \mid Q_1$. Hence we have $P_n \xrightarrow{n} P_1$, which can only be matched by $Q_n \xrightarrow{n} Q_1$, so we have $P_1 \dot{\sim}_l Q_1$.

We suppose now that $n.\mathbf{0}$ is under a locality in P_n and Q_n. We prove that $n.\mathbf{0}$ is under the same hierarchy of localities in P_n, Q_n, and the existence of the pairwise bisimilar processes defined in the lemma. Suppose $n.\mathbf{0}$ is under k localities $a_1, \dots a_k$ in P_n and under l localities $b_1, \dots b_l$ in Q_n, with $k > l$. We have $P_n \xrightarrow{a_1} \langle P'_1\{n.\mathbf{0}/X_i\} \rangle P_1$, so there exists Q_1, Q'_1 such that $Q_n \xrightarrow{b_i}$

$\langle Q'_1\{n.\mathbf{0}/X_j\}\rangle Q_1$ with $a_1 = b_i$ and $P'_1\{n.\mathbf{0}/X_i\} \dot{\sim}_l Q'_1\{n.\mathbf{0}/X_j\}$. The process is under $k-1$ localities in P'_1 and under $l-i$ localities in Q'_1, with $i \geq 1$. After l passivation, we have P'_l such that the process $n.\mathbf{0}$ is under $k-l$ localities, and a process Q'_l such that the process $n.\mathbf{0}$ is not under a locality and with $P'_l \dot{\sim}_l Q'_l$, which is not possible (same proof as in the first case). If $k < l$, we have a similar contradiction by reasoning on Q, consequently we have $k = l$.

Therefore there exists $a_1 \dots a_k$, $P_1 \dots P_k$, $Q_1 \dots Q_k$, such that $P_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$ and $Q_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$. Let P'_i (resp Q'_i) be the process inside the locality a_i in P_n (resp Q_n). We have $P_n \xrightarrow{\overline{a_1}} \langle P'_1\rangle P_1$, with $P'_1 \xrightarrow{n}$, which is matched by a passivation $Q_n \xrightarrow{\overline{a_i}} \langle Q'_i\rangle Q'$ such that $P_1 \dot{\sim}_l Q'$, $P'_1 \dot{\sim}_l Q'_i$ and $Q'_i \xrightarrow{n}$. If $i \neq 1$, we have the process under $k-1$ localities in P'_1 and in $k-i < k-1$ localities in Q'_i, with $P'_i \dot{\sim}_l Q'_i$: contradiction. Hence we have $i = 1$, $P_1 \dot{\sim}_l Q' = Q_1$ and $P'_1 \dot{\sim}_l Q'_1$. By induction on $1 \leq j \leq k$, we have $P_j \dot{\sim}_l Q_j$ and $P'_k = n.\mathbf{0} \mid P_{k+1} \dot{\sim}_l n.\mathbf{0} \mid Q_{k+1} = Q'_k$. Since the reduction $P'_k \xrightarrow{n} P_{k+1}$ can only be matched $Q'_k \xrightarrow{n} Q_{k+1}$, we have $P_{k+1} \dot{\sim}_l Q_{k+1}$, consequently we have the required result.

□

In the following, we write X_i the i-th occurrence of X in a process P.

Lemma 41. *Let P, Q two open processes such that $fv(P,Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. Let R, R' two closed processes such that $R \dot{\sim}_l R'$. Suppose we have $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} = P_n$ is matched by the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\} = Q_n$ (with $P_n \dot{\sim}_l Q_n$). Then we have the relation $P'\{m.n.\mathbf{0}/X\}\{R/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$.*

Proof. By lemma 40, we have two cases to consider:

- Suppose we have $P_n = n.\mathbf{0} \mid P_1$, $Q_n = n.\mathbf{0} \mid Q_1$ with $P_1 \dot{\sim}_l Q_1$. Since $P_1 \dot{\sim}_l Q_1$, $R \dot{\sim}_l R'$ and $\dot{\sim}_l$ is a congruence we have $R \mid P_1 \dot{\sim}_l R' \mid Q_1$ by transitivity, consequently the result holds.
- Suppose we have $P_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$ and $Q_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$ and for all $1 \leq j \leq k+1$, $P_j \dot{\sim}_l Q_j$. Since $P_{k+1} \dot{\sim}_l Q_{k+1}$, $R \dot{\sim}_l R'$, $\dot{\sim}_l$ is a congruence and is transitive, we have $R \mid P_{k+1} \dot{\sim}_l R' \mid Q_{k+1}$. So we have $a_k[R \mid P_{k+1}] \mid P_k \dot{\sim}_l a_k[R' \mid Q_{k+1}] \mid Q_k$. By induction on $1 \leq j \leq k$, we have $a_j[\dots a_k[R \mid P_{k+1}] \mid P_k \dots] \mid P_j \dot{\sim}_l a_j[\dots a_k[R' \mid Q_{k+1}] \mid Q_k \dots] \mid Q_j$, so we have the required result with $j = 1$.

□

Theorem 12. *Let P, Q two open processes such that $fv(P,Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. If $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, then for all closed processes R, we have $P\{R/X\} \dot{\sim}_l Q\{R/X\}$*

Proof. We show that the relation $\mathcal{R} = \{(P\{R/X\}, Q\{R/X\}), P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}, m, n \text{ not in } P, Q\}$ is a strong bisimulation. Since the relation is symmetrical, it is enough to prove that it is a simulation. We make a case analysis on the transition from $P\{R/X\}$:

The transition comes only from P. We have $P\{R/X\} \xrightarrow{\alpha} A\{R/X\}$ with $P \xrightarrow{\alpha} A$. Hence we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} A\{m.n.\mathbf{0}/X\}$. We distinguish the three cases for A:

- Process case P'. Since $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists Q' such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} Q'$ and $P'\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q'$. Since m does not occur in P, Q, we have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} Q'$ comes only from Q. Therefore Q' can be written $Q' = Q''\{m.n.\mathbf{0}/X\}$ for some Q'', and we have $Q\{R/X\} \xrightarrow{\alpha} Q''\{R/X\}$. We have $P'\{R/X\} \mathcal{R} Q''\{R/X\}$, hence the result holds.

- Abstraction case F. Since $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists F' such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} F'$ and $(F\{m.n.\mathbf{0}/X\}) \circ T \dot{\sim}_l F' \circ T$ for all processes T. Since the transition is on a higher-order name, we have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} F'$ comes only from Q. Therefore F' can be written $F' = F''\{m.n.\mathbf{0}/X\}$ for some F'', and we have $Q\{R/X\} \xrightarrow{\alpha} F''\{R/X\}$. Since T is a closed process, we have $(F\{R/X\}) \circ T = (F \circ T)\{R/X\} \mathcal{R} (F'' \circ T)\{R/X\} = (F''\{R/X\}) \circ T$, hence the result holds.

- Concretion case $C = \langle T \rangle S$. Since $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists $C' = \langle T' \rangle S'$ such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} C'$, $T\{m.n.\mathbf{0}/X\} \dot{\sim}_l T'$ and $S\{m.n.\mathbf{0}/X\} \dot{\sim}_l S'$. We have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} C'$ comes only from Q. Therefore T', S' can be written $T' = T''\{m.n.\mathbf{0}/X\}$ and $S' = S''\{m.n.\mathbf{0}/X\}$ for some T'', S'', and we have $Q\{R/X\} \xrightarrow{\alpha} (\langle T'' \rangle S'')\{R/X\}$. We have $T\{R/X\} \mathcal{R} T''\{R/X\}$ and $S\{R/X\} \mathcal{R} S''\{R/X\}$, hence the result holds.

The transition comes only from R. A copy of R is in an evaluation context and perform a transition. We write X_i the occurrence of X where the copy of R performs the transition. We have $P\{R/X\} \xrightarrow{\alpha} P'\{R/X\}\{A/X_i\}$ with $R \xrightarrow{\alpha} A$. Since X_i is in an evaluation context, we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\}$. Since we have $P\{m.n.\mathbf{0}/X\} \dot{\sim}_l Q\{m.n.\mathbf{0}/X\}$, there exists a transition $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$ (an occurrence of X, noted X_j, is in an evaluation context in Q) with $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$. Consequently we have $Q\{R/X\} \xrightarrow{\alpha} Q'\{R/X\}\{A/X_j\}$.

We distinguish three cases for A:

- Process case R'. We have $P'\{m.n.\mathbf{0}/X\}\{R'/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$ by lemma 41, so we have $P'\{R/X\}\{R'/X_i\} \mathcal{R} Q'\{R/X\}\{R'/X_j\}$ as required.

- Abstraction case F. By lemma 41, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_j\}$ for all T. We have $(P'\{R/X\}\{F/X_i\}) \circ T = P'\{R/X\}\{F \circ T/X_i\} \mathcal{R} Q'\{R/X\}\{F \circ T/X_i\} = (Q'\{R/X\}\{F/X_j\}) \circ T$ as required.

- Concretion case $\langle S \rangle T$. By lemma 41, we have $P'\{m.n.\mathbf{0}/X\}\{T/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{T/X_j\}$, so we have $P'\{R/X\}\{T/X_i\} \mathcal{R} Q'\{R/X\}\{T/X_j\}$. Moreover we have $S \dot{\sim}_l S$, and since $\dot{\sim}_l \subseteq \mathcal{R}$ (with P, Q closed processes), we have $S \mathcal{R} S$ and $P'\{R/X\}\{T/X_i\} \mathcal{R} Q'\{R/X\}\{T/X_j\}$ as required.

A higher-order communication takes place between R and P. A copy of R is in an evaluation context and communicate with a sub-process P' of P. We have two cases to consider.

The first possibility is $R \xrightarrow{a} F$ and $P' \xrightarrow{\overline{a}} \langle T\{R/X\} \rangle S\{R/X\}$ for some a. We have the transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{F \circ (T\{R/X\})\} \mid \mathbb{E}_{3,R}\{S\{R/X\}\}\}$$

for some evaluation contexts $\mathbb{E}_{1,R}, \mathbb{E}_{2,R}, \mathbb{E}_{3,R}$ (the subscript R means that occurrences of X in the context are filled with R). We have

$$\begin{aligned} P\{m.n.\mathbf{0}/X\} &\xrightarrow{m}\xrightarrow{\overline{a}} \\ &\langle T\{m.n.\mathbf{0}/X\} \rangle \mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\} \end{aligned}$$

so by bisimilarity hypothesis, there exists $T', \mathbb{E}'$ such that we have

$$Q\{m.n.\mathbf{0}/X\} \xrightarrow{m}\xrightarrow{\overline{a}} \langle T'\{m.n.\mathbf{0}/X\} \rangle \mathbb{E}'_{m.n.\mathbf{0}}\{n.\mathbf{0}\}$$

and the messages and continuations are bisimilar, i.e. we have

$$T\{m.n.\mathbf{0}/X\} \dot{\sim}_l T'\{m.n.\mathbf{0}/X\}$$

and

$$\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\} \dot{\sim}_l \mathbb{E}'_{m.n.\mathbf{0}}\{n.\mathbf{0}\}$$

From the relation on messages, we have

$$F \circ (T\{m.n.\mathbf{0}/X\}) \dot{\sim}_l F \circ (T'\{m.n.\mathbf{0}/X\})$$

Hence by lemma 41 and the relation on continuations, we have

$$\begin{aligned} &\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{F \circ (T\{m.n.\mathbf{0}/X\})\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\} \\ &\qquad \dot{\sim}_l \mathbb{E}'_{m.n.\mathbf{0}}\{F \circ (T'\{m.n.\mathbf{0}/X\})\} \end{aligned}$$

We have $Q\{R/X\} \xrightarrow{\tau} \mathbb{E}'_R\{F \circ (T'\{R/X\})\}$ and

$$\mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{F \circ (T\{R/X\})\} \mid \mathbb{E}_{3,R}\{S\{R/X\}\}\} \mathcal{R} \mathbb{E}'_R\{F \circ (T'\{R/X\})\}$$

hence the result holds.

The second possibility is $R \xrightarrow{\overline{a}} \langle T \rangle S$ and $P' \xrightarrow{a} F\{R/X\}$ for some a. We have the transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{S\} \mid \mathbb{E}_{3,R}\{(F\{R/X\}) \circ T\}\}$$

for some evaluation contexts $\mathbb{E}_{1,R}, \mathbb{E}_{2,R}, \mathbb{E}_{3,R}$. We have the transitions

$$P\{m.n.\mathbf{0}/X\} \xrightarrow{m}\xrightarrow{a} \mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{F\{m.n.\mathbf{0}/X\}\}\}$$

so there exists F' such that

$$Q\{m.n.\mathbf{0}/X\} \xrightarrow{m}\xrightarrow{a} \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{F'\{m.n.\mathbf{0}/X\}\}\}$$

for some contexts and we have

$$\begin{aligned}&\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{(F\{m.n.\mathbf{0}/X\}) \circ T\}\}\\ &\qquad \dot{\sim}_l \; \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{(F'\{m.n.\mathbf{0}/X\}) \circ T\}\}\end{aligned}$$

By lemma 41, we have the relation

$$\begin{aligned}&\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{S\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{(F\{m.n.\mathbf{0}/X\}) \circ T\}\}\\ &\qquad \dot{\sim}_l \; \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{S\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{(F'\{m.n.\mathbf{0}/X\}) \circ T\}\}\end{aligned}$$

We have $Q\{R/X\} \xrightarrow{\tau} \mathbb{E}'_{1,R}\{\mathbb{E}'_{2,R}\{S\} \mid \mathbb{E}'_{3,R}\{(F'\{R/X\}) \circ T\}\}$ and

$$\begin{aligned}&\mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{S\} \mid \mathbb{E}_{3,R}\{(F\{R/X\}) \circ T\}\}\\ &\qquad \mathcal{R} \; \mathbb{E}'_{1,R}\{\mathbb{E}'_{2,R}\{S\} \mid \mathbb{E}'_{3,R}\{(F'\{R/X\}) \circ T\}\}\end{aligned}$$

hence the result holds.

A first-order communication takes place between R and P. This case is similar to the case above.

A higher-order communication takes place between two copies of R. Two copies of R are in evaluation contexts and communicate. There exists $F, \langle T \rangle S$ such that $R \xrightarrow{a} F$ and $R \xrightarrow{\overline{a}} \langle T \rangle S$ for some a. We note X_i, X_j the two occurrences of X in P where the transitions are performed: the transition can be written $P\{R/X\} \xrightarrow{\tau} P''\{R/X\}\{F \circ T/X_i\}\{S/X_j\}$.

We have $P\{R/X\} \xrightarrow{a} P'\{R/X\}\{F/X_i\}$. Since X_i is in an evaluation context, we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\}$, so there exists Q' such that $Q\{m.n.\mathbf{0}/X\} \xrightarrow{m} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_k\}$ and $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_k\}$. Since $F \circ T \dot{\sim}_l F \circ T$, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \dot{\sim}_l Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}$ by lemma 41.

Since X_j is in an execution context, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \xrightarrow{m} P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{n.\mathbf{0}/X_j\}$. Consequently by the previous equivalence there exists Q'' such that $Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\} \xrightarrow{m} Q''\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}\{n.\mathbf{0}/X_l\}$ and $P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{n.\mathbf{0}/X_j\} \dot{\sim}_l Q''\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}\{n.\mathbf{0}/X_l\}$. Since $S \dot{\sim}_l S$, by lemma 41 we have $P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{S/X_j\} \dot{\sim}_l Q''\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}\{S/X_l\}$. We have $Q\{R/X\} \xrightarrow{\tau} Q''\{R/X\}\{F \circ T/X_k\}\{S/X_l\}$ and the relation $P''\{R/X\}\{F \circ T/X_i\}\{S/X_j\}\ \mathcal{R}\ Q''\{R/X\}\{F \circ T/X_k\}\{S/X_l\}$, hence the result holds.

A first-order communication takes place between two copies of R. This case is similar to the case above.

□

F.2 Weak case

Lemma 42. *Let P, Q such that there exists P', Q' such that $Q \overset{\tau}{\Rightarrow} Q'$, $P \overset{\tau}{\Rightarrow} P'$, $P \dot{\approx}_l Q'$ and $Q \dot{\approx}_l P'$. Then we have $P \dot{\approx}_l Q$.*

Proof. Suppose we have $P \not\dot{\approx}_l Q$. We have two cases to consider. We suppose first that there exists an action α and an agent A such that $P \xrightarrow{\alpha} A$, and the transition is not matched by Q. Since we have $P \dot{\approx}_l Q'$, there exists $Q' \overset{\alpha}{\Rightarrow} B$ such that $A \dot{\approx}_l B$. Hence we have $Q \overset{\tau}{\Rightarrow} Q' \overset{\alpha}{\Rightarrow} B$, i.e. $Q \overset{\alpha}{\Rightarrow} B$ such that $A \dot{\approx}_l B$: we have a matching transition from Q, contradiction.

The other possibility is an action from Q not matched by P. The proof is similar using $Q \dot{\approx}_l P'$. □

Lemma 43. *Let P, Q two open processes such that $fv(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. Suppose we have $P\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} = P_n$ matched by $Q\{m.n.\mathbf{0}/X\} \overset{m}{\Rightarrow} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\} = Q_n$. Then we are in one of the following cases:*

- *There exists P_1, Q_1 such that $P_n = n.\mathbf{0} \mid P_1$, $Q_n = n.\mathbf{0} \mid Q_1$ with $P_1 \dot{\approx}_l Q_1$.*
- *There exists $a_1, \ldots a_k$, $P_1 \ldots P_{k+1}$, $Q_1 \ldots Q_{k+1}$ such that*

  $$P_n = a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \ldots] \mid P_1$$

  and

  $$Q_n = a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \ldots] \mid Q_1$$

  There exists $P'_1, \ldots P'_{k+1}$, $Q'_1, \ldots Q'_{k+1}$ such that

  $$P_n \overset{\tau}{\Rightarrow} a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid P'_{k+1}] \mid P'_k] \mid P'_{k-1} \ldots] \mid P'_1$$

  and

  $$Q_n \overset{\tau}{\Rightarrow} a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid Q'_{k+1}] \mid Q'_k] \mid Q'_{k-1} \ldots] \mid Q'_1$$

  and for all $1 \leq j \leq k+1$, we have $P_j \dot{\approx}_l Q'_j$ and $P'_j \dot{\approx}_l Q_j$.

Proof. The proof is similar to the strong case one. We just detail the differences.

Suppose $n.\mathbf{0}$ is not under a locality in P_n. Then it is not under a locality in Q_n, and there exists P_1, Q_1 such that $P_n = n.\mathbf{0} \mid P_1$ and $Q_n = n.\mathbf{0} \mid Q_1$. We have $P_n \xrightarrow{n} P_1$, hence there exists Q'_1 such that $Q_n \stackrel{n}{\Rightarrow} Q'_1$ and $P_1 \dot{\approx}_l Q'_1$. Since Q_n may perform only one $\xrightarrow{n}$ transition, we have in fact $Q_1 \stackrel{\tau}{\Rightarrow} Q'_1$. Similarly, there exists P'_1 such that $P_n \stackrel{\tau}{\Rightarrow} P'_1$ and $Q_1 \dot{\approx}_l P'_1$. By Lemma 42, we have $P_1 \dot{\approx}_l Q_1$ as required.

Suppose now $n.\mathbf{0}$ is under the locality hierarchy $a_1 \dots a_k$ in P_n. Then it is under the same hierarchy in Q_n. There exists $P_1 \dots P_{k+1}$, $Q_1 \dots Q_{k+1}$ such that $P_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$ and $Q_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$. Let T_i (resp U_i) be the process inside the locality a_i in P_n (resp Q_n). We have $P_n \xrightarrow{\overline{a_1}} \langle T_1 \rangle P_1$, with $T_1 \xrightarrow{n}$, which can only be matched by $Q_n \stackrel{\overline{a_1}}{\Longrightarrow} \langle U'_i \rangle S'$, $S' \stackrel{\tau}{\Rightarrow} Q'_1$, $T_1 \dot{\approx}_l U'_1$ and $P_1 \dot{\approx}_l Q'_1$. More precisely, we have $Q_n \stackrel{\tau}{\Rightarrow} a_1[U'_1] \mid S' \xrightarrow{\overline{a_1}} \langle U'_1 \rangle S'$ and $S' \stackrel{\tau}{\Rightarrow} Q'_1$, hence we have $Q_n \stackrel{\tau}{\Rightarrow} a_1[U'_1] \mid Q'_1$ (using LTS-Par).

From $T_1 \dot{\approx}_l U'_1$ we build similarly U'_2, Q'_2 such that $T_2 \dot{\approx}_l U'_2$, $P_2 \dot{\approx}_l Q'_2$ and $Q_n \stackrel{\tau}{\Rightarrow} a_1[a_2[U'_2] \mid Q'_2] \mid Q'_1$. By induction on $1 \leq j \leq k$, there exists Q'_j, U'_j such that $P_j \dot{\approx}_l Q'_j$ and $Q_n \stackrel{\tau}{\Rightarrow} a_1[\dots a_j[U'_j] \mid Q'_j \dots] \mid Q'_1$ and $T_k = n.\mathbf{0} \mid P_{k+1} \dot{\approx}_l n.\mathbf{0} \mid Q'_{k+1} = U'_k$. The reduction $T_k \xrightarrow{n} P_{k+1}$ is matched by $U'_k \stackrel{n}{\Rightarrow} Q''_{k+1}$ with $P_{k+1} \dot{\approx}_l Q''_{k+1}$. Since U'_k may perform only one $\xrightarrow{n}$ transition, we have in fact $Q'_{k+1} \stackrel{\tau}{\Rightarrow} Q''_{k+1}$. Similarly by considering the transition $U'_k \xrightarrow{n} Q'_{k+1}$, we can build P'_{k+1} such that $P_{k+1} \stackrel{\tau}{\Rightarrow} P'_{k+1}$ and $Q'_{k+1} \dot{\approx}_l P'_{k+1}$. Hence by lemma 42, we have $P_{k+1} \dot{\approx}_l Q'_{k+1}$.

Finally, we have $Q_n \stackrel{\tau}{\Rightarrow} a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q'_{k+1}] \mid Q'_k] \mid Q'_{k-1} \dots] \mid Q'_1$ with $P_j \dot{\approx}_l Q'_j$ for all $1 \leq j \leq k+1$ as required. By reasonning on transitions from Q_n, we build similarly $P'_1, \dots P'_{k+1}$ such that $P_n \stackrel{\tau}{\Rightarrow} a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P'_{k+1}] \mid P'_k] \mid P'_{k-1} \dots] \mid P'_1$ and $P'_j \dot{\approx}_l Q_j$ for all $1 \leq j \leq k+1$.

□

Lemma 44. *Let P, Q two open processes such that $fv(P,Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. Let R, R' two closed processes such that $R \dot{\approx}_l R'$. Suppose we have $P\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q\{m.n.\mathbf{0}/X\}$ and $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} = P_n$ is matched by the transition $Q\{m.n.\mathbf{0}/X\} \stackrel{m}{\Rightarrow} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\} = Q_n$ (with $P_n \dot{\approx}_l Q_n$). Then we have the relation $P'\{m.n.\mathbf{0}/X\}\{R/X_i\} \dot{\approx}_l Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$.*

Proof. By lemma 43, we have two cases to consider:

- Suppose we have $P_n = n.\mathbf{0} \mid P_1$, $Q_n = n.\mathbf{0} \mid Q_1$ with $P_1 \dot{\approx}_l Q_1$. Since $P_1 \dot{\approx}_l Q_1$, $R \dot{\approx}_l R'$ and $\dot{\approx}_l$ is a congruence we have $R \mid P_1 \dot{\approx}_l R' \mid Q_1$ by transitivity, consequently the result holds.
- Suppose we have $P_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1$ and $Q_n = a_1[\dots a_{k-1}[a_k[n.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1$ and $P_n \stackrel{\tau}{\Rightarrow}$

$a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid P'_{k+1}] \mid P'_k] \mid P'_{k-1}\ldots] \mid P'_1$ and $Q_n \stackrel{\tau}{\Rightarrow} a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid Q'_{k+1}] \mid Q'_k] \mid Q'_{k-1}\ldots] \mid Q'_1$ with $P_j \mathrel{\dot{\approx}_l} Q'_j$ and $P'_j \mathrel{\dot{\approx}_l} Q_j$ for all $1 \leq j \leq k+1$.

Since $P_{k+1} \mathrel{\dot{\approx}_l} Q'_{k+1}$, $R \mathrel{\dot{\approx}_l} R'$, $\dot{\approx}_l$ is a congruence and is transitive, we have $R \mid P_{k+1} \mathrel{\dot{\approx}_l} R' \mid Q'_{k+1}$. Hence we have $a_k[R \mid P_{k+1}] \mid P_k \sim_l a_k[R' \mid Q'_{k+1}] \mid Q'_k$. By induction on $1 \leq j \leq k$, we have $a_j[\ldots a_k[R \mid P_{k+1}] \mid P_k\ldots] \mid P_j \mathrel{\dot{\approx}_l} a_j[\ldots a_k[R' \mid Q'_{k+1}] \mid Q'_k\ldots] \mid Q'_j$. With $j = 1$, we have $P'\{m.n.\mathbf{0}/X\}\{R/X_i\} \mathrel{\dot{\approx}_l} a_1[\ldots a_{k-1}[a_k[R \mid Q'_{k+1}] \mid Q'_k] \mid Q'_{k-1}\ldots] \mid Q'_1$. From $Q_n \stackrel{\tau}{\Rightarrow} a_1[\ldots a_{k-1}[a_k[n.\mathbf{0} \mid Q'_{k+1}] \mid Q'_k] \mid Q'_{k-1}\ldots] \mid Q'_1$, we have $Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\} \stackrel{\tau}{\Rightarrow} a_1[\ldots a_{k-1}[a_k[R' \mid Q'_{k+1}] \mid Q'_k] \mid Q'_{k-1}\ldots] \mid Q'_1$.

Similarly, we have $P'\{m.n.\mathbf{0}/X\}\{R/X_i\} \stackrel{\tau}{\Rightarrow} a_1[\ldots a_{k-1}[a_k[R \mid P'_{k+1}] \mid P'_k] \mid P'_{k-1}\ldots] \mid P'_1$ and $a_1[\ldots a_{k-1}[a_k[R \mid P'_{k+1}] \mid P'_k] \mid P'_{k-1}\ldots] \mid P'_1 \mathrel{\dot{\approx}_l} Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$. Consequently we can apply lemma 42 and we have $P'\{m.n.\mathbf{0}/X\}\{R/X_i\} \mathrel{\dot{\approx}_l} Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$ as required.

□

Lemma 45. *Let P be an open process with fv$(P) \subseteq \{X\}$ and m, n be names which do not occur in P. If $P\{m.n.\mathbf{0}/X\} \stackrel{m}{\Rightarrow} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$ where X_j is in an evaluation context, then for all R such that $R \xrightarrow{\alpha} A$, we have $P\{R/X\} \stackrel{\alpha}{\Rightarrow} P'\{R/X\}\{A/X_j\}$.*

Proof. The transition $P\{m.n.\mathbf{0}/X\} \stackrel{m}{\Rightarrow} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$ may be decomposed in $P\{m.n.\mathbf{0}/X\} \stackrel{\tau}{\Rightarrow}\xrightarrow{m} P_1\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\} \stackrel{\tau}{\Rightarrow} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$. Since m, n do not occur in P, the τ-action between P_1, P' do not involve synchronisations on m, n. Consequently the transition may be rewritten in $P\{m.n.\mathbf{0}/X\} \stackrel{\tau}{\Rightarrow} P_1\{m.n.\mathbf{0}/X\}\{m.n.\mathbf{0}/X_j\} \stackrel{\tau}{\Rightarrow} P'\{m.n.\mathbf{0}/X\}\{m.n.\mathbf{0}/X_j\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$. Using the same transitions, we have $P\{R/X\} \stackrel{\tau}{\Rightarrow} P'\{R/X\}\{R/X_j\} \xrightarrow{\alpha} P'\{R/X\}\{A/X_j\}$, hence we have the required result.

□

Theorem 13. *Let P, Q two open processes such that fv$(P, Q) \subseteq \{X\}$ and m, n two names which do not occur in P, Q. If $P\{m.n.\mathbf{0}/X\} \mathrel{\dot{\approx}_l} Q\{m.n.\mathbf{0}/X\}$, then for all closed processes R, we have $P\{R/X\} \mathrel{\dot{\approx}_l} Q\{R/X\}$*

Proof. We show that the relation $\mathcal{R} = \{(P\{R/X\}, Q\{R/X\}), P\{m.n.\mathbf{0}/X\} \mathrel{\dot{\approx}_l} Q\{m.n.\mathbf{0}/X\}, m, n \text{ not in } P, Q\}$ is a weak bisimulation. Since the relation is symmetrical, it is enough to prove that it is a simulation. We make a case analysis on the transition from $P\{R/X\}$:

The transition comes only from P. We have $P\{R/X\} \xrightarrow{\alpha} A\{R/X\}$ with $P \xrightarrow{\alpha} A$. Hence we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{\alpha} A\{m.n.\mathbf{0}/X\}$. We distinguish the three cases for A:

- Process case P'. Since $P\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q\{m.n.\mathbf{0}/X\}$, there exists Q' such that $Q\{m.n.\mathbf{0}/X\} \stackrel{\alpha}{\Rightarrow} Q'$ and $P'\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q'$. Since m does not occur in P, Q, we have $\alpha \neq m$, so the transitions $Q\{m.n.\mathbf{0}/X\} \stackrel{\alpha}{\Rightarrow} Q'$ comes only from Q. Therefore Q' can be written $Q' = Q''\{m.n.\mathbf{0}/X\}$ for some Q'', and we have $Q\{R/X\} \stackrel{\alpha}{\Rightarrow} Q''\{R/X\}$. We have $P'\{R/X\} \mathcal{R} Q''\{R/X\}$, hence the result holds.

- Abstraction case F. Since $P\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q\{m.n.\mathbf{0}/X\}$, there exists F' such that $Q\{m.n.\mathbf{0}/X\} \stackrel{\alpha}{\Rightarrow} F'$, and for all T, there exists Q' such that $F' \circ T \stackrel{\tau}{\Rightarrow} Q'$ and $(F\{m.n.\mathbf{0}/X\}) \circ T \dot{\approx}_l Q'$. Since the transition is on a higher-order name, we have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \stackrel{\alpha}{\Rightarrow} F'$ comes only from Q. Therefore F', Q' can be written $F' = F''\{m.n.\mathbf{0}/X\}$ and $Q' = Q''\{m.n.\mathbf{0}/X\}$ for some F'', Q'', and we have $Q\{R/X\} \stackrel{\alpha}{\Rightarrow} F''\{R/X\}$ and $F''\{R/X\} \circ T \stackrel{\tau}{\Rightarrow} Q''\{R/X\}$. Since T is a closed process, we have $(F\{R/X\}) \circ T = (F \circ T)\{R/X\} \mathcal{R} Q''\{R/X\}$, hence the result holds.

- Concretion case $C = \langle T \rangle S$. Since $P\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q\{m.n.\mathbf{0}/X\}$, there exists $C' = \langle T' \rangle U$, S' such that $U \stackrel{\tau}{\Rightarrow} S'$, $Q\{m.n.\mathbf{0}/X\} \stackrel{\alpha}{\Rightarrow} C'$, $T\{m.n.\mathbf{0}/X\} \dot{\approx}_l T'$ and $S\{m.n.\mathbf{0}/X\} \dot{\approx}_l S'$. We have $\alpha \neq m$, so the transition $Q\{m.n.\mathbf{0}/X\} \stackrel{\alpha}{\Rightarrow} C'$ comes only from Q. Therefore T', U, S' can be written $T' = T''\{m.n.\mathbf{0}/X\}$, $U = U'\{m.n.\mathbf{0}/X\}$, and $S' = S''\{m.n.\mathbf{0}/X\}$ for some T'', U', S'', and we have $Q\{R/X\} \stackrel{\alpha}{\Rightarrow} (\langle T'' \rangle U')\{R/X\}$ and $U'\{R/X\} \stackrel{\tau}{\Rightarrow} S''\{R/X\}$. We have $T\{R/X\} \mathcal{R} T''\{R/X\}$ and $S\{R/X\} \mathcal{R} S''\{R/X\}$, hence the result holds.

The transition comes only from R. A copy of R is in an evaluation context and perform a transition. We write X_i the occurrence of X where the copy of R performs the transition. We have $P\{R/X\} \xrightarrow{\alpha} P'\{R/X\}\{A/X_i\}$ with $R \xrightarrow{\alpha} A$. Since X_i is in an evaluation context, we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\}$. Since $P\{m.n.\mathbf{0}/X\} \dot{\approx}_l Q\{m.n.\mathbf{0}/X\}$, there exists a $Q\{m.n.\mathbf{0}/X\} \stackrel{m}{\Rightarrow} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$ such that $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \dot{\approx}_l Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$ (an occurrence of X, noted X_j, is in an evaluation context in Q) with $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \dot{\approx}_l Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_j\}$. By lemma 45, we have $Q\{R/X\} \stackrel{\alpha}{\Rightarrow} Q'\{R/X\}\{A/X_j\}$.

We distinguish three cases for A:

- Process case R'. We have $P'\{m.n.\mathbf{0}/X\}\{R'/X_i\} \dot{\approx}_l Q'\{m.n.\mathbf{0}/X\}\{R'/X_j\}$ by lemma 44, so we have $P'\{R/X\}\{R'/X_i\} \mathcal{R} Q'\{R/X\}\{R'/X_j\}$ as required.

- Abstraction case F. By lemma 44, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \dot{\approx}_l Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_j\}$ for all T. We have $(P'\{R/X\}\{F/X_i\}) \circ T = P'\{R/X\}\{F \circ T/X_i\} \mathcal{R} Q'\{R/X\}\{F \circ T/X_i\} = (Q'\{R/X\}\{F/X_j\}) \circ T$ as required.

- Concretion case $\langle S\rangle T$. By lemma 41, we have $P'\{m.n.\mathbf{0}/X\}\{T/X_i\} \dot{\approx}_l Q'\{m.n.\mathbf{0}/X\}\{T/X_j\}$, so we have $P'\{R/X\}\{T/X_i\} \mathcal{R}\, Q'\{R/X\}\{T/X_j\}$. Moreover we have $S \dot{\approx}_l S$, and since $\dot{\approx}_l \subseteq \mathcal{R}$ (with P, Q closed processes), we have $S\, \mathcal{R}\, S$ and $P'\{R/X\}\{T/X_i\} \mathcal{R}\, Q'\{R/X\}\{T/X_j\}$ as required.

A higher-order communication takes place between R and P. A copy of R is in an evaluation context and communicate with a sub-process P' of P. We have two cases to consider.

The first possibility is $R \xrightarrow{a} F$ and $P' \xrightarrow{\overline{a}} \langle T\{R/X\}\rangle S\{R/X\}$ for some a. We have the transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{F \circ (T\{R/X\})\} \mid \mathbb{E}_{3,R}\{S\{R/X\}\}\}$$

for some evaluation contexts $\mathbb{E}_{1,R}, \mathbb{E}_{2,R}, \mathbb{E}_{3,R}$. We have

$$\begin{aligned}&P\{m.n.\mathbf{0}/X\}\\ &\quad\xrightarrow{m}\xrightarrow{\overline{a}} \langle T\{m.n.\mathbf{0}/X\}\rangle \mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\}\end{aligned}$$

so by bisimilarity hypothesis, there exists T', E', $\mathbb{E}'$ such that $Q\{m.n.\mathbf{0}/X\} \overset{m}{\Rightarrow}\overset{\overline{a}}{\Rightarrow} \langle T'\{m.n.\mathbf{0}/X\}\rangle E'$, $E' \overset{\tau}{\Rightarrow} \mathbb{E}'_{m.n.\mathbf{0}}\{n.\mathbf{0}\}$, and the messages and continuations are bisimilar, i.e.

$$T\{m.n.\mathbf{0}/X\} \dot{\approx}_l T'\{m.n.\mathbf{0}/X\}$$

and

$$\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\} \dot{\approx}_l \mathbb{E}'_{m.n.\mathbf{0}}\{n.\mathbf{0}\}$$

From the relation on messages and the congruence properties of $\dot{\approx}_l$, we have

$$F \circ (T\{m.n.\mathbf{0}/X\}) \dot{\approx}_l F \circ (T'\{m.n.\mathbf{0}/X\})$$

Using this relation and the one on continuations, we have

$$\begin{aligned}&\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{F \circ (T\{m.n.\mathbf{0}/X\})\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{S\{m.n.\mathbf{0}/X\}\}\}\\ &\qquad\qquad\dot{\approx}_l \mathbb{E}'_{m.n.\mathbf{0}}\{F \circ (T'\{m.n.\mathbf{0}/X\})\}\end{aligned}$$

by lemma 44. We have $Q\{R/X\} \overset{\tau}{\Rightarrow} \mathbb{E}'_R\{F \circ (T'\{R/X\})\}$ and

$$\mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{F \circ (T\{R/X\})\} \mid \mathbb{E}_{3,R}\{S\{R/X\}\}\}\ \mathcal{R}\ \mathbb{E}'_R\{F \circ (T'\{R/X\})\}$$

hence the result holds.

The second possibility is $R \xrightarrow{\overline{a}} \langle T\rangle S$ and $P' \xrightarrow{a} F\{R/X\}$ for some a. We have the transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{S\} \mid \mathbb{E}_{3,R}\{(F\{R/X\}) \circ T\}\}$$

for some evaluation contexts $\mathbb{E}_{1,R}, \mathbb{E}_{2,R}, \mathbb{E}_{3,R}$. We have the transitions

$$P\{m.n.\mathbf{0}/X\} \xrightarrow{m} \xrightarrow{a} \mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{F\{m.n.\mathbf{0}/X\}\}\}$$

matched by $Q\{m.n.\mathbf{0}/X\}$. There exists F', Q' such that

$$Q\{m.n.\mathbf{0}/X\} \stackrel{m}{\Rightarrow} \stackrel{a}{\Rightarrow} \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{F'\{m.n.\mathbf{0}/X\}\}\}$$

with

$$\mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{F'\{m.n.\mathbf{0}/X\} \circ T\}\} \stackrel{\tau}{\Rightarrow} \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{Q'\{m.n.\mathbf{0}/X\}\}\}$$

and

$$\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{(F\{m.n.\mathbf{0}/X\}) \circ T\}\} \mathrel{\dot{\approx}_l} \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{n.\mathbf{0}\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{(Q'\{m.n.\mathbf{0}/X\})\}\}$$

By lemma 44, we have

$$\mathbb{E}_{1,m.n.\mathbf{0}}\{\mathbb{E}_{2,m.n.\mathbf{0}}\{S\} \mid \mathbb{E}_{3,m.n.\mathbf{0}}\{(F\{m.n.\mathbf{0}/X\}) \circ T\}\} \mathrel{\dot{\approx}_l} \mathbb{E}'_{1,m.n.\mathbf{0}}\{\mathbb{E}'_{2,m.n.\mathbf{0}}\{S\} \mid \mathbb{E}'_{3,m.n.\mathbf{0}}\{(Q'\{m.n.\mathbf{0}/X\})\}\}$$

We have $Q\{R/X\} \stackrel{\tau}{\Rightarrow} \mathbb{E}'_{1,R}\{\mathbb{E}'_{2,R}\{S\} \mid \mathbb{E}'_{3,R}\{(F'\{R/X\}) \circ T\}\}$ and

$\mathbb{E}_{1,R}\{\mathbb{E}_{2,R}\{S\} \mid \mathbb{E}_{3,R}\{(F\{R/X\}) \circ T\}\} \mathrel{\mathcal{R}} \mathbb{E}'_{1,R}\{\mathbb{E}'_{2,R}\{S\} \mid \mathbb{E}'_{3,R}\{(Q'\{R/X\})\}\}$

hence the result holds.

A first-order communication takes place between R and P. This case is similar to the case above.

A higher-order communication takes place between two copies of R. Two copies of R are in evaluation contexts and communicate. There exists $F, \langle T\rangle S$ such that $R \xrightarrow{a} F$ and $R \xrightarrow{\overline{a}} \langle T\rangle S$ for some a. We note X_i, X_j the two occurrences of X in P where the transitions are performed: the transition can be written $P\{R/X\} \xrightarrow{\tau} P''\{R/X\}\{F \circ T/X_i\}\{S/X_j\}$.

We have $P\{R/X\} \xrightarrow{a} P'\{R/X\}\{F/X_i\}$. Since X_i is in an evaluation context, we have $P\{m.n.\mathbf{0}/X\} \xrightarrow{m} P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\}$, so there exists Q' such that $Q\{m.n.\mathbf{0}/X\} \stackrel{m}{\Rightarrow} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_k\}$ and $P'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_i\} \mathrel{\dot{\approx}_l} Q'\{m.n.\mathbf{0}/X\}\{n.\mathbf{0}/X_k\}$. Since $F \circ T \mathrel{\dot{\approx}_l} F \circ T$, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \mathrel{\dot{\approx}_l} Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}$ by lemma 44.

Since X_j is in an execution context, we have $P'\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\} \xrightarrow{m} P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{n.\mathbf{0}/X_j\}$. Consequently by the previous equivalence there exists Q'' such that $Q'\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\} \stackrel{m}{\Rightarrow} Q''\{m.n.\mathbf{0}/X\}\{F \circ$

$T/X_k\}\{n.\mathbf{0}/X_l\}$ and $P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{n.\mathbf{0}/X_j\} \dot{\approx}_l Q''\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}\{n.\mathbf{0}/X_l\}$. Since $S \dot{\approx}_l S$, by lemma 44 we have $P''\{m.n.\mathbf{0}/X\}\{F \circ T/X_i\}\{S/X_j\} \dot{\approx}_l Q''\{m.n.\mathbf{0}/X\}\{F \circ T/X_k\}\{S/X_l\}$. We have $Q\{R/X\} \stackrel{\tau}{\Rightarrow} Q''\{R/X\}\{F \circ T/X_k\}\{S/X_l\}$ and the relation $P''\{R/X\}\{F \circ T/X_i\}\{S/X_j\} \mathcal{R} Q''\{R/X\}\{F \circ T/X_k\}\{S/X_l\}$, hence the result holds.

A first-order communication takes place between two copies of R. This case is similar to the case above.

□

G Abstraction equivalence in HOπP

We remind the definition of finite processes:

Definition 36. *A finite process is a HOπP process built on the following grammar:*

$$P_F ::= \mathbf{0} \;\mid\; P_F \mid P_F \;\mid\; l.P_F \;\mid\; \nu x.P_F \;\mid\; \overline{a}\langle P\rangle P_F \;\mid\; a(X)P_F \;\mid\; a[P_F]$$

A concretion $\nu\widetilde{x}.\langle R\rangle S$ is finite iff S is finite. An abstraction $(X)P$ is finite iff P is finite. We write A_F the set of finite agents.

We first prove some properties on finite processes:

Lemma 46. *Let F be a finite abstraction. For all process P, $F \circ P$ is finite.*

Proof. We have $F = (X)P_F$ for some finite process P_F, hence $F \circ P = P_F\{P/X\}$. Since P_F is finite, X appears in messages only, hence after substitution, P appears in messages only. Since any processes are allowed as messages, $F \circ P$ is a finite process.

□

Lemma 47. *Let P_F be a finite process. If $P_F \xrightarrow{\alpha} A$ for some α, then A is finite.*

Proof. By induction on P_F:

- $P_F = 0$: no available transition.
- $P_F = P_1 \mid P_2$, where P_1 and P_2 are finite processes. The possible transitions come from rules LTS-Par, LTS-FO, LTS-HO, and their symmetric. In the LTS-Par case, we have $P_1 \xrightarrow{\alpha} A$, and $P_F \xrightarrow{\alpha} A \mid P_2$. By induction, A is finite, hence $A \mid P_2$ is finite. The proof is similar for the symmetric rule.

  In the LTS-FO case, we have $P_1 \xrightarrow{m} P_1'$, $P_2 \xrightarrow{\overline{m}} P_2'$, and $P_F \xrightarrow{\tau} P_1' \mid P_2'$. By induction, P_1' and P_2' are finite, hence so is $P_1' \mid P_2'$. In the LTS-HO case, we have $P_1 \xrightarrow{\overline{a}} C = \nu\widetilde{x}.\langle R\rangle S$, $P_2 \xrightarrow{a} F$, and $P_F \xrightarrow{\tau} F \bullet C$. By induction, F and S are finite. By lemma 46, $F \circ R$ is finite, hence $\nu\widetilde{x}.(F \circ R \mid S) = F \bullet C$ is finite.

- $P_F = l.P'$, where P' is finite. The possible transition comes from rule LTS-PREFIX $P_F \xrightarrow{l} P'$. Since P' is finite, the result holds.
- $P_F = \nu x.P'$, where P' is finite. The possibles transitions come from rule LTS-RESTR: we have $P_F \xrightarrow{\alpha} \nu x.A$ with $P' \xrightarrow{\alpha} A$. By induction, A is finite, hence $\nu x.A$ is finite.
- $P_F = \overline{a}\langle R\rangle S$, where S is finite. The possible transition comes from rule LTS-CONCR $P_F \xrightarrow{\overline{a}} \langle R\rangle S$. Since S is finite, $\langle R\rangle S$ is finite.
- $P_F = a(X)P'$, where P' is finite. The possible transition comes from rule LTS-ABSTR $P_F \xrightarrow{a} (X)P'$. Since P' is finite, $(X)P'$ is finite.
- $P_F = a[P']$, where P' is finite. The possible transitions comes from rules LTS-PASSIV and LTS-LOC. In the LTS-PASSIV case, we have $P_F \xrightarrow{\overline{a}} \langle P'\rangle\mathbf{0}$. Since $\mathbf{0}$ is finite, $\langle P'\rangle\mathbf{0}$ is finite. In the LTS-LOC case, we have $P' \xrightarrow{\alpha} A$ and $P_F \xrightarrow{\alpha} a[A]$. By induction, A is finite, hence $a[A]$ is finite.

□

Lemma 48. *Let P_F be a finite process.*

- *The set $\{\alpha | \exists A, P_F \xrightarrow{\alpha} A\}$ is finite.*
- *For all action α, the set $\{A | P_F \xrightarrow{\alpha} A\}$ is finite.*

Proof. Easy by induction on P_F. □

We now prove that a finite process "terminates". To this end, we introduce the *size* of a finite process P_F, written $s(P_F)$, defined inductively as:

$$s(\mathbf{0}) = 0 \quad s(P_1 \mid P_2) = s(P_1) + s(P_2) \quad s(l.P) = 1 + s(P) \quad s(\nu x.P) = s(P)$$

$$s(\overline{a}\langle R\rangle S) = 1 + s(S) \quad s(a(X)P) = 1 + s(P) \quad s(a[P]) = 1 + s(P)$$

The size of a finite concretion $\nu\widetilde{x}.\langle R\rangle P_F$ is defined by $s(C) = s(P_F)$, and the size of a finite abstraction $F = (X)P_F$ is defined by $s(F) = s(P_F)$. By definition, the size of an agent is a non-negative integer.

Lemma 49. *Let F be a finite abstraction. For all processes P, we have $s(F \circ P) = s(F)$.*

Proof. We have $F = (X)P_F$ for some finite process P_F, hence $F \circ P = P_F\{P/X\}$. Since P_F is finite, X appears in messages only, hence after substitution, P appears in messages only. Since the size of a message output depends only on the size of the continuation, we have $s(F \circ P) = s(F)$.

□

Lemma 50. *Let P_F be a finite process. If $P_F \xrightarrow{\alpha} A$, then $s(P_F) > s(A)$.*

Proof. By induction on P_F:

- $P_F = 0$: no available transition.
- $P_F = P_1 \mid P_2$, where P_1 and P_2 are finite processes. The possible transitions come from rules LTS-PAR, LTS-FO, LTS-HO, and their symmetric. In the LTS-PAR case, we have $P_1 \xrightarrow{\alpha} A$, and $P_F \xrightarrow{\alpha} A \mid P_2$. By induction, we have $s(A) < s(P_1)$, hence we have $s(A \mid P_2) = s(A) + s(P_2) < s(P_1) + s(P_2) = s(P_F)$ as required.

  In the LTS-FO case, we have $P_1 \xrightarrow{m} P_1'$, $P_2 \xrightarrow{\overline{m}} P_2'$, and $P_F \xrightarrow{\tau} P_1' \mid P_2'$. By induction, $s(P_1') < s(P_1)$ and $s(P_2') < s(P_2)$, hence we have $s(P_1' \mid P_2') = s(P_1') + s(P_2') < s(P_1) + s(P_2) = s(P_F)$ as required.

  In the LTS-HO case, we have $P_1 \xrightarrow{\overline{a}} C = \nu\widetilde{x}.\langle R\rangle S$, $P_2 \xrightarrow{a} F$, and $P_F \xrightarrow{\tau} F \bullet C$. By induction, $s(F) < s(P_1)$ and $s(C) < s(P_2)$. By lemma 49, we have $s(F \circ R) = s(F)$, hence we have $s(F \bullet C) = s(F \circ R \mid S) = s(F \circ R) + s(S) = s(F) + s(S) < s(P_1) + s(P_2) = s(P_F)$ as required.
- $P_F = l.P'$, where P' is finite. The possible transition comes from rule LTS-PREFIX $P_F \xrightarrow{l} P'$. We have $s(P_F) = 1 + s(P') > s(P')$ as required.
- $P_F = \nu x.P'$, where P' is finite. The possibles transitions come from rule LTS-RESTR: we have $P_F \xrightarrow{\alpha} \nu x.A$ with $P' \xrightarrow{\alpha} A$. By induction, we have $s(A) < s(P')$ hence we have $s(\nu x.A) = s(A) < s(P') = s(P_F)$ as required.
- $P_F = \overline{a}\langle R\rangle S$, where S is finite. The possible transition comes from rule LTS-CONCR $P_F \xrightarrow{\overline{a}} \langle R\rangle S$. We have $s(P_F) = 1 + s(S) > s(S) = s(\langle R\rangle S)$ as required.
- $P_F = a(X)P'$, where P' is finite. The possible transition comes from rule LTS-ABSTR $P_F \xrightarrow{a} (X)P'$. We have $s(P_F) = 1 + s(P') > s(P') = s((X)P')$ as required.
- $P_F = a[P']$, where P' is finite. The possible transitions comes from rules LTS-PASSIV and LTS-LOC. In the LTS-PASSIV case, we have $P_F \xrightarrow{\overline{a}} \langle P'\rangle\mathbf{0}$. We have $s(P_F) = 1 + s(P') > 0 = s(\langle P'\rangle\mathbf{0})$ as required.

  In the LTS-LOC case, we have $P' \xrightarrow{\alpha} A$ and $P_F \xrightarrow{\alpha} a[A]$. We have $s(A) < s(P')$, hence we have $s(a[A]) = 1 + s(A) < 1 + s(P') = s(P_F)$ as required.

□

Lemma 51. *Let P_F be a finite process. There is no infinite sequence of processes $(P_i)_i$ such that $P_0 = P_F$ and for all i, $P_i \xrightarrow{l} P_{i+1}$ or $P_i \xrightarrow{\overline{a}} \nu\widetilde{x}.\langle R\rangle P_{i+1}$ or $P_i \xrightarrow{a} F$ with $F \circ P = P_{i+1}$ for some P.*

Proof. Suppose we have a sequence of processes $(P_i)_i$ as defined in the lemma. In this case, the sequence $(s(P_i))_i$ is an infinite sequence of strictly decreasing non-negative integers by lemma 50, which is not possible.

□

All these properties allow us to define the depth of a finite process:

Definition 37. *We define inductively the depth of a finite agent A_F, written $d(A_F)$, as:*

- $d(P_F) = 0$ *if there is no transition from* P_F.
- $d(P_F) = 1 + \max\{d(A) | \exists\alpha, P_F \xrightarrow{\alpha} A\}$ *otherwise.*
- *For all finite concretions* $\nu\widetilde{x}.\langle P\rangle P_F$, *we have* $d(\nu\widetilde{x}.\langle P\rangle P_F) = d(P_F)$.
- *For all finite abstractions* $(X)P_F$, *we have* $d(F) = d(P_F)$.

We now prove that testing a finite process is not enough. We define:

$$F_0 \triangleq (X_0)X_0, G_0 \triangleq (X_0)(X_0 \mid X_0)$$

and for $n > 0$, we define

$$F_n \triangleq (X_n)\nu a_n.(a_n[X_n] \mid a_n.F_{n-1}) + R_n$$

$$G_n \triangleq (X_n)\nu a_n.(a_n[X_n] \mid a_n.G_{n-1}) + S_n$$

with $R_n = \nu a_n.\tau.G_{n-1} \circ X_n$ and $S_n = \nu a_n.\tau.F_{n-1} \circ X_n$.

Let (m_k) be a family of pairwise distinct fresh names which do not occur in any F_n nor G_n. Let $Q_1 = m_1.\mathbf{0}$ and $Q_{k+1} = m_{k+1}.Q_k$ for all $k > 1$.

Let P_F be a finite process such that $d(P_F) = 0$. Consequently P_F cannot perform any transition, and $P_F \mid P_F$ neither. Hence we have $P_F \sim P_F \mid P_F$, i.e. $F_0 \circ P_F \sim G_0 \circ P_F$.

We now prove that $F_n \circ P_F \sim G_n \circ P_F$ for all P_F such that $d(P_F) \leq n$, for $n > 0$. We define:

$$\mathcal{R}_n \triangleq \{(P\{\widetilde{F_k \circ P_k}/\widetilde{X}\}, P\{\widetilde{G_k \circ P_k}/\widetilde{X}\}), \forall k, d(P_k) \leq k \leq n\}$$

Lemma 52. *The relation $\mathcal{R}_n$ is a bisimulation.*

Proof. Let $(P_1, P_2) \in \mathcal{R}_n$. We discuss on the possible transitions from P_1:

- Transitions from P which do not involve any $F_k \circ P_k$. These are matched by the same transitions in P_2.
- Passivation of locality a_{k_0} in a process $F_{k_0} \circ P_{k_0}$, i.e. we have $P_1 \xrightarrow{\tau} P\{\nu a_{k_0}.F_{k_0-1} \circ P_{k_0}/X_0\}\{\widetilde{F_k \circ P_k}/\widetilde{X} \setminus X_0\} = P_1'$ (the variable X_0 is in an evaluation context). We distinguish two cases. We suppose first that $d(P_{k_0}) \leq k_0 - 1$. In P_2, we perform passivation of a_{k_0} in $G_{k_0} \circ P_{k_0}$, i.e. $P_2 \xrightarrow{\tau} P\{\nu a_{k_0}.F_{k_0-1} \circ P_{k_0}/X_0\}\{\widetilde{G_k \circ P_k}/\widetilde{X} \setminus X_0\} = P_2'$. We rewrite P_1' in $P'\{\widetilde{F_k \circ P_k}/\widetilde{X}\}$ and P_2' in $P'\{\widetilde{G_k \circ P_k}/\widetilde{X}\}$ (P' differs from P only in the restriction on a_{k_0}). Since we have $d(P_{k_0}) \leq k_0 - 1 \leq n$, we have $P_1' \mathcal{R}_n P_2'$.

We suppose now that $d(P_{k_0}) = k_0$. In P_2, we perform the τ-action in the sub-process $S_{k_0} \circ P_{k_0}$ of $G_{k_0} \circ P_{k_0}$, i.e. we have $P_2 \xrightarrow{\tau} P\{\nu a_{k_0}.F_{k_0-1} \circ P_{k_0}/X_0\}\{\widetilde{G_k \circ P_k}/\widetilde{X} \setminus X_0\} = P'_2$. Let $P' = P\{\nu a_{k_0}.F_{k_0-1} \circ P_{k_0}/X_0\}$; we rewrite P'_1 in $P'\{\widetilde{F_k \circ P_k}/\widetilde{X} \setminus X_0\}$ and P'_2 in $P'\{\widetilde{G_k \circ P_k}/\widetilde{X} \setminus X_0\}$. Consequently we have $P'_1 \mathcal{R}_n P'_2$.

- Internal action from sub-process $R_{k_0} \circ P_{k_0} \xrightarrow{\tau} \nu a_{k_0}.G_{k_0-1} \circ P_{k_0}$ in a process $F_{k_0} \circ P_{k_0}$, i.e. we have $P_1 \xrightarrow{\tau} P\{\nu a_{k_0} G_{k_0-1} \circ P_{k_0}./X_0\}\{\widetilde{F_k \circ P_k}/\widetilde{X} \setminus X_0\} = P'_1$. In P_2, we perform passivation of a_{k_0} in $G_{k_0} \circ P_{k_0}$, i.e. $P_2 \xrightarrow{\tau} P\{\nu a_{k_0}.G_{k_0-1} \circ P_{k_0}/X_0\}\{\widetilde{G_k \circ P_k}/\widetilde{X} \setminus X_0\} = P'_2$. Let $P' = P\{\nu a_{k_0}.G_{k_0-1} \circ P_{k_0}/X_0\}$; we rewrite P'_1 in $P'\{\widetilde{F_k \circ P_k}/\widetilde{X} \setminus X_0\}$ and P'_2 in $P'\{\widetilde{G_k \circ P_k}/\widetilde{X} \setminus X_0\}$. Consequently we have $P'_1 \mathcal{R}_n P'_2$.

- First order action $P_{k_0} \xrightarrow{l} P'$ in a process $F_{k_0} \circ P_{k_0}$, i.e. we have $P_1 \xrightarrow{l} P\{\widetilde{F_k \circ P_k}, F_{k_0} \circ P'/\widetilde{X}\} = P'_1$. We perform the same action in P_2, i.e. $P_2 \xrightarrow{l} P\{\widetilde{G_k \circ P_k}, G_{k_0} \circ P'/\widetilde{X}\} = P'_2$. Since we have $d(P') \leq d(P_{k_0}) - 1 \leq k_0 \leq n$, we have $P'_1 \mathcal{R}_n P'_2$ as required.

- Higher-order input $P_{k_0} \xrightarrow{a} F$ in a process $F_{k_0} \circ P_{k_0}$, i.e. we have $P_1 \xrightarrow{a} P\{\widetilde{F_k \circ P_k}, F_{k_0} \circ F/\widetilde{X}\} = F_1$ (with a little abuse of notation). Let $C = \nu\widetilde{x}.\langle R\rangle S$ be a closed concretion. We perform the same action in P_2, i.e. $P_2 \xrightarrow{a} P\{\widetilde{G_k \circ P_k}, G_{k_0} \circ F/\widetilde{X}\} = F_2$. We have $F_1 \bullet C = \nu\widetilde{x}.(S \mid P\{\widetilde{F_k \circ P_k}, F_{k_0} \circ (F \circ R)/\widetilde{X}\})$, which we rewrite in $P'\{\widetilde{F_k \circ P_k}, F_{k_0} \circ (F \circ R)/\widetilde{X}\}$. Similarly, we have $F_2 \bullet C = P'\{\widetilde{G_k \circ P_k}, G_{k_0} \circ (F \circ R)/\widetilde{X}\}$. We have $d(F \circ R) = d(F) \leq d(P_{k_0}) - 1 \leq k_0 \leq n$, hence we have $F_1 \bullet C \mathcal{R}_n F_2 \bullet C$ as required.

- Higher-order output $P_{k_0} \xrightarrow{\overline{a}} C = \nu\widetilde{x}.\langle R\rangle S$ in a process $F_{k_0} \circ P_{k_0}$, i.e. we have $P_1 \xrightarrow{\overline{a}} \nu\widetilde{x}.\langle R\rangle P\{\widetilde{F_k \circ P_k}, F_{k_0} \circ S/\widetilde{X}\} = C_1$. Let $F, \mathbb{E}$ be closed abstraction and evaluation context. We perform the same action in P_2, i.e. $P_2 \xrightarrow{\overline{a}} \nu\widetilde{x}.\langle R\rangle P\{\widetilde{G_k \circ P_k}, G_{k_0} \circ P'/\widetilde{X}\} = C_2$. We rewrite the process $F \bullet \mathbb{E}\{C_1\} = \nu\widetilde{x}.(F \circ R \mid \mathbb{E}\{P\{\widetilde{F_k \circ P_k}, F_{k_0} \circ S/\widetilde{X}\}\})$ in $P'\{\widetilde{F_k \circ P_k}, F_{k_0} \circ S/\widetilde{X}\}$. Similarly, we have $F \bullet \mathbb{E}\{C_2\} = P'\{\widetilde{G_k \circ P_k}, G_{k_0} \circ S/\widetilde{X}\}$. Since $d(S) = d(C) \leq d(P_{k_0}) - 1 \leq k_0 \leq n$, we have $F \bullet \mathbb{E}\{C_1\} \mathcal{R}_n F \bullet \mathbb{E}\{C_2\}$ as required.

- First-order or higher-order interaction between two processes P_{k_0} and P_{k_1} or between a process P_{k_0} and P. We deals only with the case of a higher-order interaction between two processes P_{k_0} and P_{k_1}, the other cases are similar or simpler. Suppose we have for instance $P_{k_0} \xrightarrow{a} F$ and $P_{k_1} \xrightarrow{\overline{a}} C = \nu\widetilde{x}.\langle R\rangle S$ for some a. Then we have $P_1 \xrightarrow{\tau} P'\{\widetilde{F_k \circ P_k}, F_{k_0} \circ (F \circ R), F_{k_1} \circ S/\widetilde{X}, X_0, X_1\} = P'_1$. We perform the same transition in P_2, i.e.

> $P_2 \xrightarrow{\tau} P'\{\widetilde{G_k \circ P_k}, G_{k_0} \circ (F \circ R), G_{k_1} \circ S/\widetilde{X}, X_0, X_1\} = P_2'$. We have $d(F \circ R) = d(F) \leq d(P_{k_0}) - 1 \leq k_0 \leq n$ and $d(S) = d(C) \leq d(P_{k_1}) - 1 \leq k_1 \leq n$, hence we have $P_1' \mathcal{R}_n P_2'$ as required.

Similarly, the transitions from P_2 are matched by P_1, hence $\mathcal{R}_n$ is a strong bisimulation.

□

Lemma 53. *For all n, we have $F_n \circ Q_{n+1} \not\approx G_n \circ Q_{n+1}$.*

Proof. We proceed by induction on n. For $n = 0$, we have $F_0 \circ m_1.\mathbf{0} = m_1.\mathbf{0} \not\approx m_1.\mathbf{0} \mid m_1.\mathbf{0} = G_0 \circ m_1.\mathbf{0}$ as required.

Let $n > 0$. We have $F_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.F_{n-1}) = P_1$, which can only be matched by $G_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.G_{n-1}) = P_2$. After passivation on a_n, we have $P_1 \xrightarrow{\tau} \nu a_n.(F_{n-1} \circ Q_n)$, which can only be matched by $P_2 \xrightarrow{\tau} \nu a_n.(G_{n-1} \circ Q_n)$. Since $a_n \notin \mathrm{fn}(F_{n-1} \circ Q_n)$ (resp. $a_n \notin \mathrm{fn}(G_{n-1} \circ Q_n)$), we have $\nu a_n.(F_{n-1} \circ Q_n) \sim_l F_{n-1} \circ Q_n$ (resp. $\nu a_n.(G_{n-1} \circ Q_n) \sim_l G_{n-1} \circ Q_n$). By induction hypothesis, we have $F_{n-1} \circ Q_n \not\approx G_{i-1} \circ Q_n$, hence we have $F_n \circ Q_{n+1} \not\approx G_i \circ Q_{n+1}$ as wished.

□

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399